

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/018182

International filing date: 07 December 2004 (07.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-182180  
Filing date: 21 June 2004 (21.06.2004)

Date of receipt at the International Bureau: 03 February 2005 (03.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

PCT/JP 2004/018182

09.12.2004.

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 4 年   6 月 2 1 日  
Date of Application:

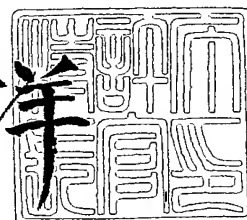
出 願 番 号            特 願 2 0 0 4 - 1 8 2 1 8 0  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 4 - 1 8 2 1 8 0 ]

出   願   人            石 井   美 恵 子  
Applicant(s):

2 0 0 5 年   1 月 2 1 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川 洋



出証番号   出証特 2 0 0 4 - 3 1 2 3 3 0 7

【書類名】 特許願  
【整理番号】 TUP0401  
【特記事項】 特許法第 4 4 条第 1 項の規定による特許出願  
【提出日】 平成16年 6月21日  
【あて先】 特許庁長官 殿  
【原出願の表示】  
    【出願番号】 特願2003-408568  
    【出願日】 平成15年12月 8日  
【国際特許分類】 G06F 17/60  
【発明者】  
    【住所又は居所】 京都府京都市下京区松原通東洞院東入本燈籠町 1 1 番地  
                        デリート烏丸東 5 0 4 号室  
    【氏名】 塚本 豊  
【特許出願人】  
    【住所又は居所】 岡山県倉敷市羽島 2 2 1 番地の 4  
    【氏名又は名称】 石井 美恵子  
【代理人】  
    【識別番号】 100104433  
    【弁理士】  
    【氏名又は名称】 宮園 博一  
【手数料の表示】  
    【予納台帳番号】 073613  
    【納付金額】 16,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1

**【書類名】特許請求の範囲****【請求項 1】**

個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップと、

前記個人ユーザが顧客またはユーザとして所定の業者に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出することができる通知用メールアドレスを生成して当該業社に通知するための処理を行うメールアドレス通知処理ステップと、

前記メールアドレス通知処理ステップにより前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成ステップと、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成ステップにより生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信ステップと、

送信元から送信された電子メールを指定されたメールアドレスに従って送信先に送信するための電子メール送信ステップと、

該電子メール送信ステップにより送信される電子メールの送信先のメールアドレスが、前記メールアドレス通知処理ステップにより通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否かを監視する監視ステップとを含むことを特徴とする、プライバシー保護方法。

**【請求項 2】**

個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護システムであって、

前記個人ユーザが顧客またはユーザとして所定の業者に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出することができる通知用メールアドレスを生成して当該業社に通知するための処理を行うメールアドレス通知処理手段と、

前記メールアドレス通知処理手段により前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段と、

送信元から送信された電子メールの送信先のメールアドレスが、前記メールアドレス通知処理手段により通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否かを監視する監視手段とを含むことを特徴とする、プライバシー保護システム。

**【請求項 3】**

前記メールアドレス通知処理手段は、メールアドレスを通知する通知業社を特定するための通知業社特定情報を含むデータを暗号化して前記通知用メールアドレスを生成する暗号化生成手段を含み、

前記監視手段は、

送信元から送信された電子メールの通知用メールアドレスを復号する復号手段と、



該復号手段により復号されたデータ中に含まれている前記通知業社特定情報と当該電子メールの送信元の情報とが一致するか否かを判定する判定手段とを含むことを特徴する、請求項 2 に記載のプライバシー保護システム。

【請求項 4】

前記通知業者は、商品を販売する販売店であり、

前記メールアドレス通知処理手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に当該販売店に対応する通知用メールアドレスを生成して通知する処理を行い、

前記発信手段は、前記販売店において購入する商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の販売価格に従って自動決済を行う際に、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、前記販売店に対応する前記通知業者用識別子を発信することを特徴とする、請求項 2 または請求項 3 に記載のプライバシー保護システム。

【請求項 5】

個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護用識別子発信装置であって、

前記個人ユーザが顧客またはユーザとなった所定の業者のために新たな通知用メールアドレスを生成して当該業社に通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【書類名】明細書

【発明の名称】プライバシー保護方法、プライバシー保護システムおよびプライバシー保護用識別子発信装置

【技術分野】

【0001】

本発明は、たとえばＩＣタグ（ＲＦＩＤタグ）等から発信されたＲＦＩＤ（Radio Frequency Identification）等の固有の識別子が読取られて該固有の識別子に基づくプライバシーの侵害を監視するための、プライバシー保護方法、プライバシー保護システムおよびプライバシー保護用識別子発信装置に関する。

【背景技術】

【0002】

メーカーで製造された商品が卸売業者等の中間流通業者に出荷された後小売店に入荷されるその商品の流通段階で当該商品を管理するために、その商品にＲＦＩＤタグを付するという提案がなされている（たとえば、特許文献１）。

【0003】

この背景技術では、メーカーからの出荷時、中間流通業者への入荷時、小売店での入荷時、消費者の購入時等の流通段階における要所要所において、商品に付されているＲＦＩＤタグに記憶されているＲＦＩＤをタグリーダが読取り、当該ＲＦＩＤが正規に登録されている適正なものであるか否かをチェックし、商品が正しく流通しているか否かを監視する。

【0004】

また、例えば、デパート等の小売店で購入したＲＦＩＤタグ付きの商品を購入者が袋に詰め、その袋を持って小売店の通過ゲートを通過する際に、その通過ゲートに設けられているタグリーダと購入商品に付されているＲＦＩＤタグとが交信し、ＲＦＩＤタグから送信されてきたＲＦＩＤに基づいて各商品の価格を自動的に割出してその合計を算出し、購入者が所持している決済機能付の携帯電話やＩＣカード等と交信して自動決済を行なう方法が提案されている（たとえば、特許文献２参照）。

【特許文献１】特開２０００－１６９２２９

【特許文献２】特開２０００－１９６５５５

【発明の開示】

【発明が解決しようとする課題】

【0005】

このように、種々の商品に付されたＲＦＩＤタグは、タグリーダからのＲＦＩＤ送信要求に応じて記憶しているＲＦＩＤを自動的に発信するために、商品が例えば衣服や眼鏡や指輪やイヤリングや腕時計等のように、常時身に付けて携帯される物の場合には、当該商品が個人ユーザに購入された後においても、タグリーダからのＲＦＩＤ送信要求に応じて当該個人ユーザが身に付けている商品のＲＦＩＤタグからＲＦＩＤが発信されることとなる。その結果、当該個人ユーザのプライバシーが侵害される虞が生ずる。

【0006】

たとえば、前述の自動決済を行うの際に、タグリーダからのＲＦＩＤ送信要求に応じて、購入者が身に付けている購入済み商品に付されているＲＦＩＤタグからもＲＦＩＤが発信されることとなる。

【0007】

その結果、たとえば或る個人ユーザであるアリスが、Ａデパートの婦人服売り場のマタニティーコーナーで岩田帯（腹帯）を購入してその商品に付されているＲＦＩＤタグをタグリーダに読み取らせて自動決済を行なった後、食器売り場で夫婦茶碗を購入してその商品に付されているＲＦＩＤタグをタグリーダに読取らせて自動決済を行なった場合には、その個人ユーザアリスが常時携帯している購入済み商品に付されているＲＦＩＤタグも同時に読み取られることとなる。そのＲＦＩＤタグのＲＦＩＤが例えば、１２３４５６であった場合には、１２３４５６のＲＦＩＤを発信するＲＦＩＤタグの商品を常時携帯してい

る同一人物が岩田帯(腹帯)を購入するとともに夫婦茶碗も購入したことがわかってしまい、その個人ユーザは、おそらく、結婚前に妊娠していることが推測できてしまう。

#### 【0008】

しかも、RFIDタグのRFIDを利用した自動決済の際に、そのAデパートのポイントカードによるポイント加算処理も合わせて行なった場合には、そのポイントカードの新規発行時にユーザ登録している個人名(アリス)や住所やEメールアドレス等の個人特定情報がつきとめられ、前述したRFID123456を発するRFIDタグを常時携帯している人物はアリスであることが見破られてしまう。

#### 【0009】

さらに、個人名、住所、Eメールアドレス等の個人特定情報と当該個人から発せられる固有の識別情報(RFID等)とが一旦リンクされ、そのリンクされた個人特定情報に前述の結婚前に妊娠している旨の個人情報が加えられたものが漏洩されて闇ルートを介して流通した場合には、次のようなプライバシーに関する深刻な問題が生じる。

#### 【0010】

たとえば、個人(アリス)が前述の漏洩された固有の識別情報を発信する発信装置(RFIDタグ等)を身に付けて外出し、たとえば書店、CDショップ、百貨店等を渡り歩き、その先々で身に付けている識別子発信装置(RFIDタグ等)が読取られてその固有の識別情報(RFID等)に基づいて前述の漏洩した個人情報が検索され、後に、たとえば、妊娠中のセックスに関する書籍の電子メール、妊娠中に適した音楽CDの電子メール、赤ちゃんのおもちゃの電子メール等の大量の迷惑メール(スパム)やダイレクトメールが届くようになる。

#### 【0011】

そこで、このような問題を防止するべく、商品購入時にその商品に付されているRFIDタグのRFID発信機能を作動不能状態に切換えるようにし、購入済商品を消費者が身につけたとしても、その商品からRFIDが発信されることがないように構成することが考えられる。

#### 【0012】

しかし、このように構成した場合には、購入済商品に付されたRFIDタグから発せられるRFIDを利用して種々のサービスを享受することができないという不都合が生ずる。購入済み商品のRFIDタグのRFIDを利用したサービスとしては、例えば、商品のRFIDタグから発せられるRFID毎に分類して当該商品の詳細な情報を登録しているサーバに消費者がRFIDのコードを送信してアクセスし、当該RFIDに対応する商品情報を検索して入手することや、商品が例えばパーソナルコンピュータ等であった場合にソフトウェアのバージョンアップ情報の提供等が考えられる。

#### 【0013】

このようなRFIDを利用したサービスを消費者が享受できるようにするためには、例えば、携帯電話等を利用して消費者自身が購入済商品に付されているRFIDタグをたとえば発信停止状態等にしてRFIDガード状態にし、かつ、RFID発信可能状態等のRFIDガード解除状態に切換えることができるように構成することが考えられる。しかし、消費者の操作等によってRFIDタグが発信状態(RFIDガード解除状態)あるいは発信停止状態(RFIDガード状態)に切換え可能にした場合には、発信停止状態(RFIDガード状態)にすべき時に消費者(個人ユーザ)が発信停止状態(RFIDガード状態)にすることを忘れて怠ってしまう虞が生ずる。その場合には、前述したプライバシーの侵害問題が発生することとなる。

#### 【0014】

また、購入済商品に付されているRFIDタグを発信停止状態や発信可能状態に切換えるための操作機能を有する新たな携帯電話等の操作装置を個人ユーザが購入しない限り、そのようなモードの切換えができないのであり、モード切換え機能を有する操作装置を有しない個人ユーザの場合には、購入済商品のRFIDタグが常にRFID発信状態つまり、常に前述したプライバシーの侵害問題が発生する状態となるという虞がある。

## 【0015】

さらに、今後RFIDタグが普及してタグリーダがいたるところに設置された場合には、いたるところで前述のプライバシー問題が頻発することになるとともに、同一コードのRFIDを追跡することにより個人ユーザの移動追跡が行なわれてしまうという虞も生じる。

## 【0016】

本発明は、係る実情に鑑み考え出されたものであり、その目的は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視することである。

## 【課題を解決するための手段】

## 【0017】

請求項1に記載の本発明は、個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップと、

前記個人ユーザが顧客またはユーザとして所定の業者に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知するための処理を行うメールアドレス通知処理ステップと、

前記メールアドレス通知処理ステップにより前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成ステップと、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成ステップにより生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信ステップと、

送信元から送信された電子メールを指定されたメールアドレスに従って送信先に送信するための電子メール送信ステップと、

該電子メール送信ステップにより送信される電子メールの送信先のメールアドレスが、前記メールアドレス通知処理ステップにより通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否かを監視する監視ステップとを含むことを特徴とする。

## 【0018】

請求項2に記載の本発明は、個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護システムであって、

前記個人ユーザが顧客またはユーザとして所定の業者に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知するための処理を行うメールアドレス通知処理手段と、

前記メールアドレス通知処理手段により前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段と、

送信元から送信された電子メールの送信先のメールアドレスが、前記メールアドレス通

知処理手段により通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否かを監視する監視手段とを含むことを特徴とする。

#### 【0019】

請求項3に記載の本発明は、請求項2に記載の発明の構成に加えて、前記メールアドレス通知処理手段は、メールアドレスを通知する通知業社を特定するための通知業社特定情報を含むデータを暗号化して前記通知用メールアドレスを生成する暗号化生成手段を含み、

前記監視手段は、

送信元から送信された電子メールの通知用メールアドレスを復号する復号手段と、

該復号手段により復号されたデータ中に含まれている前記通知業社特定情報と当該電子メールの送信元の情報とが一致するか否かを判定する判定手段とを含むことを特徴とする。

#### 【0020】

請求項4に記載の本発明は、請求項2または請求項3に記載の発明の構成に加えて、前記通知業者は、商品を販売する販売店であり、

前記メールアドレス通知処理手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に当該販売店に対応する通知用メールアドレスを生成して通知する処理を行い、

前記発信手段は、前記販売店において購入する商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の販売価格に従って自動決済を行う際に、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、前記販売店に対応する前記通知業者用識別子を発信することを特徴とする。

#### 【0021】

請求項5に記載の本発明は、個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護用識別子発信装置であって、

前記個人ユーザが顧客またはユーザとなった所定の業者のために新たな通知用メールアドレスを生成して当該業社に通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段とを含むことを特徴とする。

#### 【発明の効果】

#### 【0022】

請求項1に記載の本発明によれば、個人ユーザが所定の業社に自己のメールアドレスを通知するときに当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知する。そして、識別子の送信要求があった場合には、個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を当該個人ユーザの意思に従って他人が読取れない識別子ガード状態した上で、通知用メールアドレスを通知した相手である通知業社に対し当該通知業社に対応した通知業社用識別子を生成して毎回同じ通知業社用識別子を発信する。この状態で、仮に通知業社に通知した通知用メールアドレスと通知業社に発信した通知業社用識別子とがリンクされてその個人情報が漏洩されたとしても、自己の個人情報がどこの通知業社から漏洩されたかを次のようにして割出すことができる。

#### 【0023】

識別子の発信要求に応じて、前述の通知業社以外の者に対し識別子を発信する場合であっても、前述の通知業社用識別子を発信する旨の個人ユーザの操作があった場合には、前述の通知業社用識別子が発信される。その通知業社用識別子を受信した者がその通知業社用識別子に基づいて漏洩された個人情報を検索して該当する個人情報を割出し、その個人情報中に含まれている前述の通知用メールアドレスに基づいて電子メールを個人ユーザに送信した場合には、当該通知用メールアドレスが前述の通知業社用として新たに生成された当該通知業社用のメールアドレスであるために、その通知用メールアドレスからそれを通知した相手である通知業社を特定する情報を割出すことができる。そして、その割出した通知業社を特定する情報と電子メールを送信してきた送信元の情報とが一致するか否かを監視し、一致しない場合には、当該電子メールの送信元が前述の通知業社から漏洩された個人情報に基づいて電子メールを送信してきた可能性が高いことが明らかとなる。

#### 【0024】

このような電子メールの送信元とその電子メールの通知用メールアドレスとの整合性チェックによる監視により、どこの通知業社が個人情報を漏洩させた可能性が高いかが判明されるとともに、電子メールを送信してきた送信元が漏洩された個人情報を入手して電子メールを送信してきた可能性が高いことが判明できる。これにより、漏洩された個人情報を利用しての電子メールの送信を抑止する効果が期待できる。

#### 【0025】

請求項2に記載の本発明によれば、個人ユーザが所定の業社に自己のメールアドレスを通知するときに当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知する。そして、識別子の送信要求があった場合には、通知用メールアドレスを通知した相手である通知業社に対し当該通知業社に対応した通知業社用識別子を生成して毎回同じ通知業社用識別子を発信する。この状態で、仮に、通知業社に通知した通知用メールアドレスと通知業社に発信した通知業社用識別子とがリンクされてその個人情報が漏洩されたとしても、自己の個人情報がどこの通知業社から漏洩されたかを次のようにして割出すことができる。

#### 【0026】

識別子の発信要求に応じて、前述の通知業社以外の者に対し識別子を発信する場合であっても、前述の通知業社用識別子を発信する旨の個人ユーザの操作があった場合には、前述の通知業社用識別子が発信される。その通知業社用識別子を受信した者がその通知業社用識別子に基づいて漏洩された個人情報を検索して該当する個人情報を割出し、その個人情報中に含まれている前述の通知用メールアドレスに基づいて電子メールを個人ユーザに送信した場合には、当該通知用メールアドレスが前述の通知業社用として新たに生成された当該通知業社用のメールアドレスであるために、その通知用メールアドレスからそれを通知した相手である通知業社を特定する情報を割出すことができる。そして、その割出した通知業社を特定する情報と電子メールを送信してきた送信元の情報とが一致するか否かを監視し、一致しない場合には、当該電子メールの送信元が前述の通知業社から漏洩された個人情報に基づいて電子メールを送信してきた可能性が高いことが明らかとなる。

#### 【0027】

このような電子メールの送信元とその電子メールの通知用メールアドレスとの整合性チェックによる監視により、どこの通知業社が個人情報を漏洩させた可能性が高いかが判明されるとともに、電子メールを送信してきた送信元が漏洩された個人情報を入手して電子メールを送信してきた可能性が高いことが判明できる。これにより、漏洩された個人情報を利用しての電子メールの送信を抑止する効果が期待できる。

#### 【0028】

請求項3に記載の本発明によれば、請求項2に記載の本発明の効果に加えて、メールアドレスを通知する通知業社を特定するための通知業社特定情報を含むデータを暗号化することにより前述の通知用メールアドレスが生成され、電子メールの送信元と通知用メールアドレスとの整合性チェックによる監視においては、送信元から送信された電子メールの

通知用メールアドレスを復号し、その復号されたデータ中に含まれている通知業社特定情報と当該電子メールの送信元の情報とが一致するかを判定して整合性のチェックを行う。その結果、送信されてきた電子メールの通知用メールアドレス自体に整合性チェックのための通知業社を特定する通知業社特定情報が含まれており、復号することによりその通知業社特定情報を容易に入手することができ、整合性チェックが行い易くなる。

#### 【0029】

請求項4に記載の本発明によれば、ポイントカードの発行に伴うユーザ登録を行った販売点において購入する商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の販売価格に従って自動決済を行う際に、無線識別子発信装置の固有の識別子を読取るための識別子送信要求があった場合には、当該販売店に対応する通知業社用識別子が発信されるために、自動決済を行うことができないながらも、当該販売店から漏洩された個人情報に基づいた電子メールが送信されてきた場合に、前述の整合性チェックによる監視が可能となる。

#### 【0030】

請求項5に記載の本発明によれば、識別子の発信要求に応じて、通知業社以外の者に対し識別子を発信する場合であっても、通知業社用識別子を発信する旨の個人ユーザの操作があった場合には、通知業社用識別子が発信される。その通知業社用識別子を受信した者がその通知業社用識別子に基づいて漏洩された個人情報を検索して該当する個人情報を割出し、その個人情報中に含まれている前述の通知用メールアドレスに基づいて電子メールを個人ユーザに送信した場合には、当該通知用メールアドレスが前述の通知業社用として新たに生成された当該通知業社用のメールアドレスであるために、その通知用メールアドレスからそれを通知した相手である通知業社を特定する情報を割出すことができる。そして、その割出した通知業社を特定する情報と電子メールを送信してきた送信元の情報とが一致するか否かを監視し、一致しない場合には、当該電子メールの送信元が前述の通知業社から漏洩された個人情報に基づいて電子メールを送信してきた可能性が高いことが明らかとなる。

#### 【0031】

このような電子メールの送信元とその電子メールの通知用メールアドレスとの整合性チェックによる監視により、どこの通知業社が個人情報を漏洩させた可能性が高いかが判明されるとともに、電子メールを送信してきた送信元が漏洩された個人情報を入手して電子メールを送信してきた可能性が高いことが判明できる。これにより、漏洩された個人情報を利用しての電子メールの送信を抑止する効果が期待できる。

#### 【発明を実施するための最良の形態】

#### 【0032】

次に、本発明の実施の形態を図面に基づいて詳細に説明する。図1は、ブロードバンドを利用したネットワークシステム全体の概略を示す構成図である。広域・大容量中継網43を通じて、クレジットカード発行会社群4、加盟店契約会社群5、受信局42、加盟店群6、サプライヤ群S、NM群（ニューミドルマン群）48、電子行政群49、XMLストア50、コンテンツプロバイダ群51、信号52、携帯電話網54に接続されたゲートウェイ53、インターネットI、ユーザ宅47、認証局群46、コンビニエンスストア群2、会社群45、データセンタ44、ライフ支援センタ8、放送局41、金融機関群7等が、情報の送受信ができるように構成されている。なお、図中40は衛星（サテライト）であり、放送局41からの放送電波を中継して受信局42に電波を送るためのものである。

。

#### 【0033】

クレジットカード発行会社群4とは、たとえばSET（Secure Electronic Transaction）により決済を行なう場合のイシューとしての機能を発揮するカード発行会社である。加盟店契約会社群5は、電子モール等を構成する加盟店群6が契約している金融機関等からなる会社であり、SETにおけるアクアイアラとして機能する機関である。サプライヤ群Sとは、商品メーカー等であり、商品や情報を提供する機関のことである。NM群48



とは、サプライヤ群 S と消費者（自然人または法人）との仲立ちを行ない、たとえば消費者のショッピング等の消費行動の支援を行なうサービス業者のことである。従来の問屋や商社等の中間業者が、サプライヤ群の販売支援を行なうのに対し、この NM 群 48 は、消費者の購入支援（消費行動支援）を行なう点で相違する。NM 群 48 の具体例としては、消費者の嗜好情報や購買履歴情報や Web サイトへのアクセス履歴情報をデータベースとして蓄積し、その蓄積されている消費者のプロフィール情報（個人情報）に基づいてその消費者にマッチする商品情報等を推薦して、消費者の消費行動を助けるサービス業者が当てはまる。

#### 【0034】

電子行政群 49 は、たとえば市役所や税務署あるいは中央官庁等の行政を電子化したものである。XML ストア 50 とは、XML による統一されたデータ構造によってデータを格納するとともに、必要に応じてデータの要求者に所定のデータを提供するデータベースのことである。XML ストア 50 には、ユーザの各種個人情報やユーザエージェント（エージェント用知識データを含む）を格納している。金融機関群 7 やユーザから XML ストア 50 にアクセスがあった場合には、本人認証を行なってセキュリティを保ったうえで、必要なデータを提供できるように構成されている。コンテンツプロバイダ群 51 とは、映像、文字、音等の種々のコンテンツをネットワークを通じて提供する業者群のことである。交通整理を行なうための信号機 52 も、広域・大容量中継網 43 に接続され、遠隔制御できるように構成されている。

#### 【0035】

携帯電話網 45 に接続されている基地局 55 に対し、ブラウザフォン（携帯電話）30 の電波が送信され、基地局 55、携帯電話網 45、ゲートウェイ 53、広域・大容量中継網 43 を介して、金融機関群 7、加盟店群 6、NM 群 48、電子行政群 49、XML ストア 50、コンテンツプロバイダ群 51 等にアクセスできるように構成されている。また車両 56 も同様に、基地局 55、携帯電話網 54、ゲートウェイ 53、広域・大容量中継網 54 を介して、各種サービス業者や各種機関にアクセスできるように構成されている。

#### 【0036】

認証局群 46 とは、電子証明書の発行希望者に対して本人認証をしたうえで電子証明書を発行する機関である。データセンタ 44 は、放送局 41 から電波により配信される各種データを格納、管理する機関のことである。加盟店群 6、サプライヤ群 S、NM 群 48、電子行政群 49、コンテンツプロバイダ群 51 等にユーザが所定の情報の送信を依頼した場合に、大容量のデータを送信する際には、それら各機関やサービス業者の配信するデータを一旦データセンタ 44 に格納しておき、所定の日時が来たときに放送局 41 から電波を通じてそのデータを配信し、受信局 42 で受信したデータを所定のユーザに広域・大容量中継網 43 を通じて配信する。

#### 【0037】

8 はライフ支援センターである。このライフ支援センター 8 は、ユーザの個人情報を収集し、その個人情報に基づきユーザにふさわしい夢、人生設計、職種、趣味等を推薦して、それらを実現するために必要となる各種商品や情報を提供してくれる加盟店（ニューミドルマンを含む）を推薦するサービスを行なう機関である。

#### 【0038】

なお、図 1 中二重線で示した部分は、無線 LAN、CATV、衛星、xDSL (digital subscriber line)、FTTH (fiber to the home) などである。

#### 【0039】

本実施の形態では、認証局群 46 ばかりでなく、金融機関群 7 も、電子証明書を発行する。図 1 中、19 はユーザに携帯される IC 端末であり、後述するようにユーザのプロフィール情報（個人情報）等が格納されている。

#### 【0040】

図 2 は、金融機関 7 を説明するための説明図である。金融機関 7 には、VP 管理サーバ 9、決済サーバ 10、認証用サーバ 11、データベース 12a、12b が備えられている。



。VP管理サーバ9は、仮想人物としてのバーチャルパーソン（以下、単に「VP」という）を管理するためのサーバである。VPとは、現実世界に実在しないネットワーク上で行動する仮想の人物のことであり、現実世界での実在人物であるリアルパーソン（以下、単に「RP」という）がネットワーク上で行動する際に、VPになりすましてそのVPとして行動できるようにするために誕生させた仮想人物のことである。また、後述するように、RPが、ネットワーク上で行動するときばかりでなく、現実世界で行動するときにもVPになりすましてそのVPとして行動する場合がある。

#### 【0041】

VP管理サーバ9は、後述するように、RPからVPの出生依頼があれば、そのVPの氏名や住所等の所定情報を決定してVPを誕生させ、そのVPのデータをデータベース12aに記憶させておく機能を有している。また、このVP管理サーバ9は、VP用の電子証明書を作成して発行する機能も有している。VPが売買や決済等の法律行為を行なう場合に、この電子証明書を相手方に送信することにより、仮想人物でありながら独立して法律行為を行なうことが可能となる。

#### 【0042】

認証用サーバ11は、RP用の電子証明書を作成して発行する機能を有する。金融機関7に設置されている決済サーバ10は、RPによる電子マネーやデビットカードを使用しての決済ばかりでなく、VPとして電子マネーやデビットカードを使用しての決済を行なうための処理を行なう機能も有している。

#### 【0043】

データベース12aは、RPやVPに関するデータを格納するものである。データベース12bは、広域・大容量中継網43やインターネットIに接続されているサイト（業者）を管理するためのデータを格納している。

#### 【0044】

図2に示すように、データベース12aには、RP用のデータとして、RPの氏名、住所、認証鍵KN、公開鍵KT、口座番号等が記憶されている。認証鍵とは、RPが金融機関7にアクセスしてきた場合に共通鍵暗号方式により本人認証を行なうための鍵である。公開鍵とは、公開鍵暗号方式に用いられる鍵であり、秘密鍵とペアとなっている鍵である。口座番号は、当該金融機関7においてRPが開設している口座番号のことである。

#### 【0045】

トラップ情報とは、サイト（業者）側が個人情報を収集してそれを不正に流通させた場合に、それを行なった犯人を割出すためにトラップ（罠）を仕掛けるための情報である。たとえば、VPが自己の個人情報のある業者（第1譲渡先）に譲渡する際に、その第1譲渡先特有の氏名を用いる。すなわち、VPが自己の氏名を複数種類有し、サイト（業者）ごとに使い分ける。このようなVP氏名を、便宜上トラップ型VP氏名という。このようにすれば、ダイレクトメールやEメールが業者側から送られてきた場合には、そのメールの宛名がトラップ型VP氏名となっているはずである。その送ってきたサイト（業者）が、トラップ型VP氏名から割出される第1譲渡先とは異なりかつ譲渡した自己の個人情報の開示許容範囲（流通許容範囲）を超えたサイト（業者）であった場合には、その個人情報が第1譲渡先によって不正に開示（流通）されたこととなる。このように、不正流通（不正開示）を行なった第1譲渡先を、トラップ型VP氏名から割出することができる。

#### 【0046】

なお、図2では、次郎が第2トラップ情報、第3トラップ情報、第2個人情報、第3個人情報、2つの情報を有している。次郎が、ネットワーク上で行動する場合に、この2人のVPを使い分けて行動するために、これら2種類のVP情報を金融機関7に登録している。VPの住所とは、後述するように、RPの希望するまたはRPの住所に近いコンビニエンスストア2の住所である。その結果、VPとして電子ショッピングをした場合の商品の配達先が、そのVPの住所であるコンビニエンスストア2に配達されることとなる。RPは、その配達されてきた商品をVPになりすましてコンビニエンスストア2にまで出向いて商品を引取ることが可能となる。このようにすれば、住所を手がかりにVPとRPと

の対応関係が見破られてしまう不都合が防止できる。

#### 【0047】

図2に示したトラップ情報の詳細は、図3に示されている。第1トラップ情報、第2トラップ情報、…の各トラップ情報は、サイト名（業社名）ごとに、氏名（トラップ型VP氏名）、公開鍵、Eメールアドレス、バーチャル口座番号、バーチャルクレジット番号を含んでいる。たとえば、サイト名（業者名）ABCにVPがアクセスする際には、VPの本名であるB13Pを用い、VPの秘密鍵KSBとペアの公開鍵KPB'を用い、VPの本当のEメールアドレスである○□×△×を用い、VPの本当の口座番号である2503を用い、VPの本当のクレジット番号である3288を用いる。

#### 【0048】

一方、サイト名（業者名）MTTにアクセスする（MTTで図30の自動決済を行う）場合には、VPの本名をそのVPの秘密鍵で1回暗号化したE（B13P）を、トラップ型VP氏名として用いる。秘密鍵としては、VPの本当の秘密鍵KSBをVPの本当の秘密鍵KSBで1回暗号化したEKSB（KSB）を用いる。この秘密鍵EKSB（KSB）に対する公開鍵KPBがデータベース12aに格納されている。Eメールアドレスとしては、金融機関7がトラップ型VPのために開設しているEメールアドレス△△△△△を用いる。口座番号としては、VPの本当の口座番号をVPの本当の秘密鍵で1回暗号化したE（2503）をバーチャル口座番号として用いる。クレジット番号は、VPの本当のクレジット番号をVPの本当の秘密鍵で1回暗号化したE（3288）を用いる。

#### 【0049】

さらに、サイト名（業者名）MECにアクセスする（MECで図30の自動決済を行う）場合には、VPの秘密鍵でVPの本名を2回暗号化したE2（B13P）をトラップ型VP氏名として用いる。

#### 【0050】

VPがトラップ型VP氏名E2（B13P）を用いてネットワーク上で行動する場合には、秘密鍵KSBを秘密鍵KSBで2回暗号化した2回暗号化秘密鍵E2KSB（KSB）を用いる。その2回暗号化秘密鍵とペアになっている公開鍵がKPB''である。Eメールアドレスは、金融機関7がトラップ型VP用のEメールアドレスとして開設している△△△△△を用いる。バーチャル口座番号は、VPの本当の口座番号を秘密鍵で2回暗号化したE2（2503）を用いる。クレジット番号は、VPの本当のクレジット番号をVPの秘密鍵で2回暗号化したバーチャルクレジット番号E2（3288）を用いる。

#### 【0051】

このように、サイト名（業社名）ごとに、トラップ情報の暗号回数が異なる。サイト側（業者側）に提供した個人情報というものは、ネットワーク上を流通した後最終的にはその個人情報主にEメールやダイレクトメールの形で返ってくる。この個人情報の帰還ループを利用してトラップを仕掛けて個人情報の不正流通を行なった犯人を追跡できるようにするのが、このトラップ情報の狙いである。すなわち、ユーザをネット上で追跡するトラッキング型クッキーの逆を行なうものである。

#### 【0052】

図4は、図2に示したVPの個人情報を説明する図である。第1個人情報、第2個人情報、第3個人情報、…の各個人情報は、個人情報A、個人情報B、…の複数種類の個人情報が集まって構成されている。たとえば、個人情報Aは、VPの年齢、性別、職業、年収等であり、個人情報Bは、VPの嗜好に関する情報である。

#### 【0053】

図4に示すように、各個人情報は、金融機関7の秘密鍵KSによるデジタル署名が付されている。たとえば、第1個人情報の個人情報Aは、○○△の個人情報自体に対しデジタル署名であるDKS（○○△）が付されている。

#### 【0054】

このデータベース12aに格納されている各個人情報は、後述するように、金融機関7がその真偽をチェックして正しいもののみをデータベース12aに格納し、正しいことを

認証するためのデジタル署名が付される。

#### 【0055】

図5は、XMLストア50の構成を示す図である。XMLストア50には、データベース72とそれを制御するサーバ71とが設置されている。サーバ71は、XMLストア50にアクセスしてきた者を、本人認証してアクセス制御する機能も備えている。

#### 【0056】

データベース72には、XMLで表現されたデータが格納されている。そのデータの中身は、VP情報として、VPの氏名であるたとえばB13P、VPユーザエージェント（知識データを含む）、サイト（業社）別情報として、サイト名（業社名）たとえばABC、そのサイト（業社）にアクセスしたVPに発行された電子証明書、そのVPの個人情報と当該サイト（業社）のプライバシーポリシーとそれら両情報に対し当該VPが付したデジタル署名DKSB（個人情報+ポリシー）と当該サイト（業社）ABCが付したデジタル署名DKSA（個人情報+ポリシー）と、トラップ情報としての暗号化回数「0」と、当該VPのEメールアドレスである○□×△×が含まれている。さらに、VPがサイト名（業社名）MTTにアクセスした場合には、そのサイト名（業社名）MTTにアクセスしたトラップ型VPに対し発行された電子証明書と、そのサイト（業社）にトラップ型VPが提供した個人情報とそのサイト（業社）のプライバシーポリシーとそれら両情報に対する当該トラップ型VPのデジタル署名と当該サイト（業社）のデジタル署名と、トラップ情報としての暗号回数「1」とEメールアドレスとが含まれている。

#### 【0057】

さらに、氏名がNPXAの他のVPの情報も、前述と同様の項目がデータベース72に記憶される。このデータベース72には、非常に多くのVPごとに、前述した項目でデータが記憶されている。

#### 【0058】

なお、サイト名（業社名）ABCについては、図3で説明したように、トラップ情報として1回も暗号化していない情報を用いているために、データベース72に格納されている暗号回数も「0」となっている。サイト名（業社名）MTTについて言えば、図3で説明したように、トラップ情報として1回暗号化した情報を用いているために、データベース72に記憶されている暗号化回数も「1」となっている。

#### 【0059】

前述したVPユーザエージェントとは、ユーザであるVPのために動作する自立型ソフトウェアのことである。このVPユーザエージェントは、ネットワークを通して移動できるようにモバイルエージェントで構成されている。

#### 【0060】

なお、図2～図5に示した各データは、暗号化した状態で各データベースに格納しておいてもよい。そうすれば、万一データが盗まれたとしても、解読できないために、セキュリティ上の信頼性が向上する。一方、たとえばVP（トラップ型VPを含む）がネットワーク上で目に余る不正行為（たとえば刑法に違反する行為）を行なった場合には、所定機関（たとえば警察等）からの要請等に応じて、そのVPをデータベース12a等から検索してそのVPに対応するRPを割出し、RPの住所氏名等を要請のあった所定機関（たとえば警察等）に提供するようにしてもよい。

#### 【0061】

図6は、コンビニエンスストア2の構成を示す図である。コンビニエンスストア2には、データベース75と、それに接続されたサーバ74と、そのサーバに接続された端末73とが設置されている。データベース75には、当該コンビニエンスストアに住所を持つVP（トラップ型VPを含む）の氏名と、それら各氏名に対応して、商品の預かり情報、Eメールアドレス、顧客管理情報等が記憶されている。

#### 【0062】

当該コンビニエンスストア2にB13PのVPが購入した商品が配達されれば、データベース75のB13Pの記憶領域に、商品預かり情報として「ABC会社からの商品預か

り、未決済」が格納される。この未決済とは、B13Pがネットを通じて商品を購入したもののまだ支払を行っていない状態のことである。

#### 【0063】

データベース75のEメールアドレスの欄には、各VPに対応してEメールアドレスが格納されている。B13Pの場合には、トラップ型VPでないために、当該VPの本当のEメールアドレスである○□×△×が格納されている。

#### 【0064】

トラップ型VPであるE(B13P)も同様に、商品預かり情報としてたとえば「MTT会社からの商品預かり、決済済」が格納される。なお、E(B13P)は、トラップ型VPであるために、Eメールアドレスは、金融機関7のトラップ型VPのために開設されているEメールアドレスが格納される。

#### 【0065】

サーバ74は、後述するように、コンビニエンスストア2にVP(トラップ型VPを含む)として商品を引取りに来た顧客が、当該コンビニエンスストア2に登録されているVP(トラップ型VPを含む)に対し商品を預かっている場合にはその商品をVP(トラップ型VPを含む)に引渡すための処理を行なう。

#### 【0066】

コンビニエンスストア2は、商品の預かりサービスばかりでなくVP用のダイレクトメールの預かりサービスも行なう。VPはコンビニエンスストア2が住所でありVP宛のダイレクトメールはコンビニエンスストア2に郵送されるためである。

#### 【0067】

図7は、ユーザに用いられる端末の一例のブラウザフォン30を示す正面図である。ブラウザフォン30には、マイクロコンピュータ199が備えられている。このマイクロコンピュータ199には、CPU(Central Processing Unit)197と、I/Oポート198と、ROM195と、EEPROM194と、RAM196とが備えられている。このブラウザフォン30は、USB(Universal Serial Bus)ポートを備えており、USBポートに対し、IC端末19Rまたは19Vまたは19Iが差込み可能に構成されている。IC端末19Rは、RP用のIC端末である。IC端末19Vは、VP用のIC端末である。IC端末19Iは、後述するように金融機関が発行したVP用のデータやプログラムが格納されてユーザにまで配達されてくるものであり、その配達されてきたIC端末19Iをブラウザフォン30のUSBポートに指込むことにより、IC端末19Iに記憶されているデータやソフトウェアがブラウザフォン30に記憶されることとなる。なお、各IC端末19R、19V、19Iは、ICカードで構成してもよい。

#### 【0068】

図8は、VP用IC端末19Vを説明するための説明図である。VP用IC端末19Vは、前述したように、ブラウザフォン30のUSBポート18に対し着脱自在に構成されており、USBポート18に差込むことにより、ブラウザフォン30との情報がやり取りできるようになり、使用可能な状態となる。

#### 【0069】

VP用IC端末19V内には、LSIチップ20が組込まれている。このLSIチップ20には、制御中枢としてのCPU24、CPU24の動作プログラムが記憶されているROM25、CPU24のワークエリアとしてのRAM22、電氣的に記憶データを消去可能なEEPROM26、コプロセッサ23、外部とのデータの入出力を行なうためのI/Oポート21等が設けられており、それらがバスにより接続されている。

#### 【0070】

EEPROM26には、電子マネー用のプログラムであるモンデックス(リロード金額データを含む)、その他の各種アプリケーションソフト、VP用に発行された電子証明書、暗証番号、トラップ型RFIDが記憶されている。このトラップ型RFIDとは、ユーザがトラップ型VPとして行動する際にそのトラップ型VPに対応するRFIDを発信するために記憶しているRFIDである。詳しくは後述する。

## 【0071】

さらに、VP用IC端末19Vは、VPのユーザエージェントとしての機能を有しており、ユーザエージェント用知識データとして、デビットカード情報、クレジットカード情報、VPの氏名、住所、VPのEメールアドレス、VPの公開鍵KPと秘密鍵KS、RPの認証鍵KN、VPの年齢、職業等、VPの各種嗜好情報、VPの家族構成、…等の各種知識データが記憶されている。

## 【0072】

RP用IC端末19Rの場合も、図8に示したVP用IC端末19Vとほぼ同様の構成を有している。相違点といえば、EEPROM26に記録されているユーザエージェント用知識データの内容が相違する。具体的には、VPの氏名、住所の代わりにRPの氏名、住所、VPのEメールアドレスの代わりにRPのEメールアドレス、VPの公開鍵や秘密鍵の代わりにRPの公開鍵、秘密鍵、VPの年齢や職業等の代わりにRPの年齢や職業等、VPの各種嗜好情報の代わりにRPの各種嗜好情報、VPの家族構成の代わりにRPの家族構成となる。トラップ型RFIDは記憶していない。

## 【0073】

なお、VPの家族構成は、VPに対応するRPの家族がVPを誕生させている場合には、その誕生しているVPの名前や住所や年齢等のデータから構成されている。つまり、RPの家族に対応するVPの家族すなわちバーチャル家族のデータがこのVPの家族構成の記憶領域に記憶されることとなる。

## 【0074】

図9は、図8に示したトラップ型RFIDの詳細を示す図である。トラップ型RFIDの記憶領域には、VP氏名ごとに、そのVP氏名に対応するトラップ型RFIDが格納される。たとえば量販店等の業社NTTでVPとしてポイントカード等を作成する際にVPがトラップ型VP名E(B13P)を登録した場合には、その業社でショッピング等の行動を行なう際にE(B13P)に対応するトラップ型RFIDであるmttをブラウザフォン(携帯電話)30から発信する。そのために各トラップ型VPに対応させてトラップ型RFIDを記憶させている。たとえば、業社MTT内でショッピング等の行動を行なう際にE(B13P)に対応するトラップ型RFIDであるmttをブラウザフォン(携帯電話)30から発信し、トラップ型VP名E<sup>2</sup>(B13P)を登録している業社MEC内でショッピング等の行動を行なう際同じmttをブラウザフォン(携帯電話)30から発信した場合には、RFIDmttを手がかりにE(B13P)とE<sup>2</sup>(B13P)とは同一人物であることが見破られてしまう虞がある。このような不都合を防止するために、業社毎に発信するRFIDを異ならせる。

## 【0075】

また、たとえば業社MTT内でショッピング等の行動を行なう際にE(B13P)に対応するトラップ型RFIDであるmttをブラウザフォン(携帯電話)30から発信し、かつ、VP名等の個人情報を一切登録していない小売店AMPMでショッピング等の行動をする際にmttを発信し、後日小売店AMPMから電子メールまたはダイレクトメールがE(B13P)宛に送られてきた場合には、E(B13P)の個人情報が業社MTTから小売店AMPMに不正に横流しされたことになる。そのような横流しを監視することができる。

## 【0076】

なお、IC端末19V、19RのEEPROM26には、公開鍵KP、秘密鍵KS、認証鍵KN、暗証番号のみを記憶させ、それ以外の情報はすべてXMLストア50の方に記憶させて必要に応じて検索して利用できるようにしてもよい。また、公開鍵KP、秘密鍵KSを用いた暗号化や復号処理は、IC端末19V、19R自体が行うのではなく、ブラウザフォン30あるいは後述するパーソナルコンピュータ30'が行うようにしてもよい。その場合には、公開鍵KP、秘密鍵KSをブラウザフォン30あるいは後述するパーソナルコンピュータ30'に出力する必要がある。

## 【0077】

図10は、携帯装置1の機能の概略を示すブロック図である。図4を参照して、携帯装置1は、たとえば指輪の形状をしており、ユーザの身体に装着しやすい形状となっている。以下、携帯装置1をIDリング1という。IDリング1は、入浴や就眠時も常時身につけることを原則とし、このことにより紛失や盗難を防ぐことができる。また、IDリング1にはセキュリティ用のRFIDタグ1aが設けられており、そのRFIDタグ1aは、RFIDタグ1aの全体を制御するためのロジック(CPU)100と、暗号化されたRFIDを記憶するための読出し専用メモリ(ROM:Read Only Memory)101と、ロジック100で実行する際に必要なランダムアクセスメモリ(RAM:Random Access Memory)102と、電気消去可能プログラマブル読出し専用メモリ(EEPROM:electrically erasable programmable read-only memory)103と、電源に用いられる電波を受信し、信号を送受信するためのループアンテナ107a、107bと、受信された電源に用いられる電波から電力を発生するための電源制御部106と、受信した信号を復調し、送信するための信号を変調するための変調・復調部105と、変調・復調部105への信号の入出力を制御するための入出力制御部104とを含む。ロジック100、ROM101、RAM102、EEPROM103、入出力制御部104は、それぞれデータバス108によって接続されている。

#### 【0078】

ロジック100は、ROM101、RAM102、EEPROM103、入出力制御部104を制御して、後述する各種処理を実行する。

#### 【0079】

ROM101は、RFIDタグ1aに付され、他のRFIDタグ1aと識別するためのRFIDとを記憶する。RFIDは、RFIDタグ1aが製造される段階、または、ユーザに発行される前の段階で記録され、その後消去されることはない。

#### 【0080】

EEPROM103には、ブラウザフォン30から送信されてきた本人認証用のパスワードが記憶される。後述するようにRFIDタグ1aを一旦発信停止状態にした後発信を再開できる状態にするときに、ブラウザフォン30からパスワードが送信され、その送信されてきたパスワードを予めEEPROM103に記憶されているパスワードと照合し一致すると判断された場合にのみ、RFIDタグ1aがRFIDを発信できる状態に切換わる。

#### 【0081】

入出力制御部104は、CPU100により制御され、変調・復調部105およびループアンテナ107aを介して情報を送受信する。これにより、RFIDタグ1aは、スキャナ(RFIDタグリーダライタ)201と無線による通信が可能である。RFIDタグ1aとスキャナ201との間の通信は、非接触型のICカードを用いた場合の通信と同様の技術が用いられる。したがって、ここではその詳細な説明は繰返さない。

#### 【0082】

一方のループアンテナ107bには大容量のコンデンサ110が接続されており、電源に用いられる電波をこのループアンテナ107bが受信してコンデンサ110に電力を貯えるように構成されている。電源に用いられる電波の送信が停止したときにこのコンデンサ110に貯えられている電力を電源制御部106に供給して引き続き所定時間(たとえば10秒程度)RFIDタグ1aが作動できるように構成されている。

#### 【0083】

図11は、図10に示したRFIDタグ1aのロジック(CPU)100の制御動作を示すフローチャートである。先ずSA1により、RFID送信指令を受信したか否かの判断がなされ、受信するまで待機する。タグリーダから電源用の電波が発せられて静電誘導によりループアンテナ107aに電力が発生した状態でロジック100が動作可能となり、その状態でタグリーダから送信されてきたRFID送信指令をループアンテナ107aが受信すれば、SA1によりYESの判断がなされてSA2へ進み、前回のRFID発信から5秒経過したか否かの判断がなされる。5秒経過していない場合にはSA10により

、前回発信したRFIDと同じものを発信する処理がなされる。5秒経過している場合には、SA3へ進み、ランダムカウンタのカウント値RをEEPROM103から読出す（抽出する）処理がなされる。このランダムカウンタは、偽RFIDのコードをランダムに生成するためのカウンタであり、後述するSA7～SA9により数値データが更新される。

#### 【0084】

次に制御がSA4へ進み、抽出したカウント値Rに基づいてテーブルを参照し、偽RFIDを割出す処理がなされる。SA4により参照されるテーブルが、図12に示されている。図12は東京都千代田区（図13参照）で販売されるRFIDタグ1aのテーブルを示しており、（a）は、1回で1つのRFIDを発信する単数発信タイプのRFIDタグ1aが記憶しているテーブルである。図12（b）、（c）は、1度に複数（例えば4個）の偽RFIDを発信する複数発信タイプのRFIDタグに記憶されているテーブルである。この複数発信タイプのRFIDタグは、複数種類製造されて販売される。そのうちの2種類のRFIDタグ1aに記憶されているテーブルを図12（b）（c）に示す。複数発信タイプのRFIDタグは、図12（b）（c）からも分かるように、ランダムカウンタの抽出値（乱数）が0～39の範囲のときに検索される4つの偽RFID1～4のうち3つの偽RFID2～4が互いに共通のコードとなっており、1つのRFID1のみ互いに異なるように構成されている。また、ランダムカウンタの抽出値（乱数）が0～39以外の範囲のときに検索される4つの偽RFID1～4は、互いに異なるバラバラなコードとなっている。一方、単数発信タイプのRFIDタグも複数種類製造販売され、ランダムカウンタの抽出値（乱数）が0～39の範囲のときに検索される偽RFIDが互いに共通のコードとなっており、ランダムカウンタの抽出値（乱数）が0～39以外の範囲のときに検索される偽RFIDが互いに異なるバラバラなコードとなっている。

#### 【0085】

前述したランダムカウンタは、SA7により「1」加算更新された後SA8によりその値が100以上になったか否かの判断がなされ、なった場合にはSA9によりランダムカウンタの値を「0」にする処理がなされる。その結果、ランダムカウンタは、0からカウントアップしてその上限である99までカウントアップされたのち、再度0からカウントアップし直すように構成されており、このようなランダムカウンタが数値データを抽出すれば、0～99の範囲内の任意の値（乱数）が抽出されることとなる。図12（a）のテーブルを記憶している単数発信タイプのRFIDタグ1aの場合には、抽出したカウント値（乱数）Rに基づいてそのテーブルを参照し、例えば抽出したランダムカウンタの値Rが0～39の範囲内の値であった場合には、820493176の偽RFIDがSA4により割出されることとなる。また、例えば抽出したランダムカウンタRの値が55～69の範囲内の数値であった場合には、813926081の偽RFIDがSA4により割出されることとなる。同様に、図12（b）に示されたテーブルを記憶している複数発信タイプのRFIDタグ1aの場合には、例えば抽出したランダムカウンタRの値が55～69の範囲内の数値であった場合には、814358231、849137655、788015233、779288401の偽RFIDがSA4により割出されることとなる。また、図12（c）に示されたテーブルを記憶している複数発信タイプのRFIDタグ1aの場合には、例えば抽出したランダムカウンタRの値が85～99の範囲内の数値であった場合には、700913561、750021214、702049319、856104923の偽RFIDがSA4により割出されることとなる。

#### 【0086】

次に制御がSA5へ進み、その割出された偽RFIDをループアンテナ107aから発信する処理がなされる。

#### 【0087】

単数発信タイプのRFIDタグ1aのそれぞれは、40%の確率で820493176の共通偽RFIDを発信し（図12（a）参照）、かつそれぞれ15%の確率で、730854709の偽RFID、813926081の偽RFID、791405731の偽



RFID、835406912等の互いにバラバラな偽RFIDを発信することとなる。その結果、このようなRFIDタグ1aを複数の個人ユーザが身に付けておれば、毎回ランダムなコードからなる偽RFIDが発信されるものの、40%という1番発信確率の高い820493176の偽RFID（以下「共通偽RFID」という）が頻繁に発信されることとなる。その結果、異なった複数場所に設置されたタグリーダによって読取られたRFIDがたまたま同一コードのRFIDであった場合には、本来なら同一人物から発信されたRFIDと判断できるが、このRFIDタグ1aが複数の個人ユーザに所持されることにより、複数箇所で同一のRFIDを受信したとしてもそれが異なる人物によって発信された前記共通偽RFIDである可能性も生じる（異人物同一識別子発信現象）。その結果、同一のRFIDを複数箇所で受信したとしても必ずしも同一人物であるとは限らないこととなり、悪意のRFID受信者側の同一人物である旨の推測を攪乱することができ、個人ユーザのプライバシーを保護することができる。

#### 【0088】

図12(a)に示すテーブルを記憶した単数発信タイプのRFIDタグ1aのみの場合には、そのRFIDタグ1aを所持する個人ユーザが他にRFIDタグを一切所持していないかあるいは所持してもRFID発信停止状態にしている場合には、前述した攪乱効果が有効に発揮される。しかし、個人ユーザが身に付けている複数の商品それぞれに付されているRFIDタグからRFIDが発信される状態となっている場合には、単数発信タイプのRFIDタグ1aを所持している状態では、タグリーダからのRFID送信指令が発せられれば、RFIDタグ1aからランダムな偽RFIDが発せられるとともに、当該個人ユーザが所持している商品に付されているRFIDタグから毎回同じRFIDが発信されることとなる。その結果、同一人物が或る場所に設置されたタグリーダに対して複数のRFIDを発信した後他の場所へ移動してそこに設置されているタグリーダに対し複数のRFIDを発信した場合には、複数のRFIDの内の一つが異なり他のものがすべて同一という現象（複数識別子中1個可変型現象）が生ずる。ただし、偶然すべてのRFIDが一致する状態となることもまれにある。その結果、一度に複数のRFIDを受信した場合には、その内の1つのRFIDが異なり他の全てが一致するかまたは全てのRFIDが一致する場合には、同一人物であると推測されてしまう不都合が生ずる。

#### 【0089】

そこで、図12(a)に示したテーブルを記憶している単数発信タイプのRFIDタグ1aばかりでなく、図12(b)、(c)に示すようなテーブルを記憶した複数発信タイプのRFIDタグ1aも合わせて製造販売して個人ユーザに普及させる。

#### 【0090】

具体的には、購入済みの所持品に付されているRFIDタグを発信停止状態等にして自己の所持品からRFIDが他人に読取れないようにしている個人ユーザには、前述の複数発信タイプのRFIDタグ1aを普及させる。一方、他人が購入済み商品からのRFIDを読取ることができるようになっている個人ユーザに対しては、前述の単数発信タイプのRFIDタグ1aを提供する。前者の個人ユーザの場合には、前述したように、1つの偽RFIDがランダムに発信されるとともに所持品に付されているRFIDタグから本物のRFIDが同時に発信されるという現象（複数識別子中1個可変型現象）が生ずる。一方、後者の個人ユーザの場合には、一度に複数（図12の場合には4個）の偽RFID1~4がランダムに発信される状態となる。ところが、前述したように、個人ユーザ同士の間で、40%の確率で共通偽RFID2~4と1つの異なったRFID1とが発信される状態となる。このような現象は、前述の複数識別子中1個可変型現象と同じ現象であるが、異なった人物の間でこの複数識別子中1個可変型現象が生ずることとなる。その結果、悪意の受信者側にしてみれば、複数識別子中1個可変型現象が生ずれば同一人物であるという推測の信頼性が低下するととなり、同一人物の推測に基づいたプライバシーの侵害が前提から崩れることとなる。

#### 【0091】

次に図11に戻り、SA6により電圧低下が生じたか否かの判断がなされる。これは、



電力用の電波の発信が停止して大容量のコンデンサ 110 に貯えられている電力を使用して R F I D タグ 1 a が作動している状態で、そのコンデンサ 110 の貯留電力が少なくなるとロジック 100 に供給される電圧が低下したか否かを判別するものである。電圧が低下したと判別された場合には、S A 10 a に進み、現時点のランダムカウンタのカウンタ値 R が E E P R O M 103 に記憶された後この偽 R F I D タグの動作がストップする。この S A 10 a により記憶されたランダムカウンタのカウンタ値 R が S A 3 により読出される（抽出される）。一方、電源用の電力が供給されている最中あるいは電源用電力がストップした後コンデンサ 110 から充分電力が供給されている最中には、S A 6 により N O の判断がなされて S A 7 以降のランダムカウンタの加算更新処理が実行されることとなる。

#### 【0092】

図 13 は、前述した複数種類の偽 R F I D タグ 1 a をグループ分けしてそのグループ毎に地域を指定して販売する地域指定方式の一例を示す説明図である。図 13 (a) は、図 12 (a) のテーブルを記憶している単数発信タイプの R F I D 1 a の地域指定の一例を示し、図 13 (b) は、図 12 (b) (c) に示された複数発信タイプの R F I D タグ 1 a の地域指定の一例を示す図である。

#### 【0093】

図 12 (a) に示された 820493176 を共通偽 R F I D として発信可能なグループに属する単数発信タイプの R F I D タグ 1 a は、図 13 (a) に示すように、東京都千代田区で販売される。また、他のグループに属する 809207321 を共通偽 R F I D として発信するグループに属する単数発信タイプの R F I D 1 a は、東京都新宿区で販売される。更に、例えば 798091320 を共通偽 R F I D として発信するグループに属する単数発信タイプの R F I D タグ 1 a は、京都市右京区で販売される。

#### 【0094】

一方、複数発信タイプの R F I D タグ 1 a の場合には、図 12 (b) (c) に示されたように、779203980, 839093127, 740980346 の 3 種類の共通偽 R F I D を 1 度に発信するグループに属する複数発信タイプの R F I D タグ 1 a は、東京都千代田区で販売される。また、他のグループに属する 788718955, 845590329, 822770945 を共通偽 R F I D として発信するグループに属する複数発信タイプの R F I D タグ 1 a は、京都市右京区で販売される。

#### 【0095】

尚、地域指定の販売方法としては、その地域内でその地域に対応するグループに属する R F I D タグ 1 a を販売するのに限らず、販売時に使用地域（例えば千代田区、新宿区、右京区等）を表示して、個人ユーザが使用しようと思っている地域の表示を見て選択して購入する方法でもよい。

#### 【0096】

このように、地域を指定して個人ユーザに提供することにより、共通偽 R F I D が一致する同一グループに属する R F I D タグ 1 a が極力同一地域内で使用されることとなり、同一地域内において同一の共通偽 R F I D が発信され易いという傾向が生じ、悪意のプライバシー侵害者を効果的に攪乱できる状態となる。

#### 【0097】

図 14 は、ブラウザフォン 30 の動作を説明するためのフローチャートである。S 95 a により、R F I D タグ切替処理がなされる。この処理は、個人ユーザが身に付けている購入済み商品に付されている R F I D タグを発信停止状態（識別子ガード状態）または発信再開状態に切替える処理である。S 95 b により、偽モード処理がなされる。この処理は、前述のセキュリティ用の R F I D タグ 1 a の偽 R F I D 発信機能をブラウザフォン 30 に持たせる処理である。S 95 c により、トラップモード処理がなされる。この処理は、個人ユーザが前述のトラップ型 V P として自動決済等を行なう場合にそのトラップ型 V P に対応する偽 R F I D を発信するための処理である。S 95 d により、R F I D 発信処理がなされる。この処理は、タグリーダから R F I D 発信要求があった場合にブラウザフ

オン 30 から R F I D を発信するための処理である。S 9 5 により、I C 端末使用モードであるか否かの判断がなされる。ブラウザフォン 30 は、R P 用 I C 端末 1 9 R または V P 用 I C 端末 1 9 V のうちのいずれか少なくとも一方を U S B ポート 1 8 に接続していなければ動作しない I C 端末使用モードと、I C 端末を接続していなくても動作可能な I C 端末未使用モードとに切換えることが可能に構成されている。そして、I C 未使用モードでない場合には S 9 6 へ進み、その他の処理がなされるが、I C 端末使用モードになっている場合には、S 9 7 へ進み、V P 用 I C 端末 1 9 V が接続されているか否かの判断がなされ、接続されていない場合には S 9 8 へ進み、R P 用 I C 端末 1 9 R が接続されているか否かの判断がなされ、接続されていない場合すなわち両 I C 端末ともに接続されていない場合には、制御は S 9 9 へ進み、I C 端末未使用の警告表示がなされた後 S 9 5 へ戻る。

#### 【0098】

一方、V P 用 I C 端末 1 9 V が接続されている場合には、制御は S 1 0 0 へ進み、自動決済処理がなされる。この処理については、図 3 1 に基づいて後述する。次に S 1 0 0 a により、ポイントカード登録処理がなされる。これは、百貨店等の業社においてポイントカードを新規発行してもらうための処理である。次に制御は S 1 0 1 へ進み、V P 出生依頼処理がなされる。次に S 1 0 2 へ進み、V P 用入力処理がなされる。次に S 1 0 3 へ進み V P 用決済処理がなされる。

#### 【0099】

次に制御が S 5 8 0 へ進み、個人情報の登録処理がなされる。この個人情報の登録処理は、図 1 8 (b) に示した V P 管理サーバ 9 の登録処理に対応するブラウザフォン 30 側の処理である。まず V P としての本人認証処理を行ない、V P 管理サーバ 9 が本人認証の確認を行なったことを条件として、V P の個人情報を金融機関 7 の V P 管理サーバ 9 へ送信してデータベース 1 2 a に登録してもらう処理を行なう。

#### 【0100】

次に制御が S 5 8 2 へ進み、個人情報の確認処理がなされる。この処理は、金融機関 7 の V P 管理サーバ 9 とブラウザフォン 30 との間でなされる処理である。まず V P としての本人認証がなされ、次に、データベース 1 2 a に格納されている自分の個人情報の確認を行なう処理がなされる。一方、確認の結果誤りがある場合あるいは引越しや転職等によって個人情報に変更があった場合には、この S 5 8 2 により、その変更情報が、金融機関 7 の V P 管理サーバ 9 へ送信される。

#### 【0101】

次に制御が S 5 8 3 へ進み、商品検索・購入処理がなされる。この処理は、図 4 5 に基づいて後述する。次に制御が S 5 8 5 へ進み、住所、氏名、E メールアドレスの送信処理が行なわれる。一方、ブラウザフォン 30 の U S B ポート 1 8 に R P 用 I C 端末 1 9 R が接続されている場合には、S 9 8 により Y E S の判断がなされて S 1 0 5 へ進み、電子証明書発行要求処理がなされる。次に制御が S 1 0 6 へ進み、R P 用入力処理がなされる。次に S 1 0 7 へ進み、R P 用決済処理がなされる。この処理については、V P 用決済処理と類似した制御処理である。

#### 【0102】

図 1 5 は、S 9 5 a に示した R F I D タグ切換え処理のサブルーチンプログラムを示すフローチャートである。S B 1 により、O F F 切換え操作があったか否かの判断がなされる。切換え操作がない場合には S B 2 へ進み、O N 切換え操作があったか否かの判断がなされる。操作がない場合にはこのサブルーチンプログラムが終了する。

#### 【0103】

一方、個人ユーザが所持している購入済み物品に付されている R F I D タグを発信停止状態にするための O F F 切換え操作がブラウザフォン 30 によりなされた場合には、S B 1 により Y E S の判断がなされて S B 3 へ進み、そのブラウザフォン 30 からパスワードが購入済み物品に付されている R F I D タグに発信される。R F I D タグはその発信されてきたパスワードを記憶する。次に S B 4 に従ってブラウザフォン 30 から O F F モード

指令が発信される。これを受けたRFIDタグは、記憶しているRFIDを発信しない状態に切換わる。これにより、RFIDタグが、個人ユーザの意思に従って他人が読取れない識別子ガード状態になる。この識別子ガード状態の他の例としては、RFIDタグをアルミ箔等で覆いRFIDを他人が読取れないようにするものであってもよい。また、RFIDタグからのRFIDの読取りを妨害する妨害電波等を送信する装置を個人ユーザが携帯し、タグリーダからのRFID読取り要求があったときに妨害電波等を送信してRFIDを読取れないようにしてもよい。次にSB5に従ってブラウザフォン30からRFIDタグへ送信指令が発信される。次にSB6へ進み、RFIDの受信があったか否かの判断がなされる。SB4に従ってOFFモード指令が既に発信されているために、通常では、個人ユーザに所持されている購入済物品に付されているRFIDタグからRFIDが発信されることはない。従って、SB6によりNOの判断がなされてSB7によりOFFモード切換え完了の表示がブラウザフォン30によりなされる。ところが、SB4によりOFFモード指令を送信したにもかかわらず、電波状況が悪かったり何らかの受信ミスが発信して個人ユーザに所持されている購入済み物品に付されているRFIDが発信停止状態に切換わらなかった場合には、SB6によりYESの判断がなされてSB8に進み、ブラウザフォン30によりエラー表示がなされる。

#### 【0104】

個人ユーザに所持されている購入済物品に付されているRFIDタグがRFID発信停止状態になった後、それを再度発信再開状態に切換えるためのON切換え操作がブラウザフォン30により行なわれた場合には、SB2によりYESの判断がなされてSB9へ進み、本人認証用のパスワードが発信される。このパスワードを受信した個人ユーザの購入済物品に付されているRFIDタグは、記憶しているパスワードと照合して一致するか否かの判断を行なって本人認証を行なう。次にブラウザフォン30は、SB12に従って、NOモード指令を送信する。これを受けた購入済物品に付されているRFIDタグは、前述したパスワードの照合によって本人認証が確認できたことを条件としてONモード指令を受信することにより、RFIDが発信可能な状態に切換わる。

#### 【0105】

次にブラウザフォン30から、SB11にしたがってRFID送信指令が発信される。次にSB12により、RFIDの受信があったか否かの判断がなされる。適正に本人認証の確認ができかつONモード指令を受信しておれば購入済物品に付されているRFIDからRFIDが発信される。その場合には、SB12によりYESの判断がなされてSB13へ進み、ONモード切換え完了表示がブラウザフォン30によりなされる。一方、本人認証が確認できなかった場合やRFID送信指令の電波を受信し損なった場合には購入済物品に付されているRFIDタグからRFIDが発信されない。その場合には、SB12よりNOの判断がなされてSB8へ進み、ブラウザフォン30によりエラー表示がなされる。

#### 【0106】

図16は、個人ユーザに所持されている購入済み物品に付されているRFIDタグの動作を示すフローチャートである。SC1により、パスワードを受信したか否かの判断がなされ、受信していない場合にはSC2へ進み、RFID送信指令を受信したか否かに判断がなされ、受信していない場合にはSC1へ戻る。このSC1→SC2→SC1のループの巡回途中でSB3またはSB9にしたがってブラウザフォン30からパスワードが発信されてくれば、SC1によりYESの判断がなされてSC3へ進む。SC3では、OFFモード指令を受信したか否かの判断がなされ、受信していない場合にはSC4へ進み、ONモード指令を受信したか否かの判断がなされ、受信していない場合にはSC3へ戻る。このSC3→SC4→SC3のループの巡回途中で、SB4にしたがってブラウザフォン30からOFFモード指令が発信されて来れば、SC3によりYESの判断がなされてSC5へ進み、受信したパスワードを記憶する処理がなされ、SC6より、OFFモードに切換える処理がなされてSC1へもどる。これにより、購入済み物品に付されているRFIDタグは、記憶しているRFIDを発信しない発信停止状態に切換わる。

## 【0107】

一方、SB10に従ってブラウザフォン30からONモード指令が発信されてくれば、SC4によりYESの判断がなされてSC7へ進み、受信したパスワードと既に記憶しているパスワードとが一致しているか否かの判断を行なって本人認証を行なう処理がなされる。一致しない場合には、本人認証の確認ができないこととなり、SC1にもどるが、一致する場合には本人認証の確認ができたと判断してSC8へ進み、ONモードに切り替える処理がなされる。これにより、購入済み物品に付されているRFIDタグは、記憶しているRFIDを発信可能な状態に切り替わる。

## 【0108】

SB5またはSB11によりブラウザフォン30からRFID発信指令があった場合あるいはタグリーダーからRFID送信指令があった場合には、SC2によりYESの判断がなされてSC9へ進み、ONモード即ち記憶しているRFIDを発信可能なモードになっているか否かの判断がなされる。ONモードになっていない場合にはSC1へ戻るが、ONモードになっている場合にはSC10へ進み、記憶しているRFIDを発信する処理がなされる。

## 【0109】

図17は、図2に示したVP管理サーバ9の処理動作を示すフローチャートである。ステップS1により、VPの出生依頼があったか否かの判断がなされる。顧客（ユーザ）がブラウザフォン30を操作してVPの出生依頼を行えば、S1aに進み、正当機関である旨の証明処理がなされる。この証明処理は、金融機関7がVPの管理をする正当な機関であることを証明するための処理であり、他人が金融機関7になりすます不正行為を防止するための処理である。この処理については、図24（b）に基づいて後述する。次にS2へ進み、RPの氏名、住所の入力要求をブラウザフォン30へ送信する。次にS3へ進み、RPの氏名、住所の返信がブラウザフォン30からあったか否かの判断がなされ、あるまで待機する。

## 【0110】

ユーザであるRPがブラウザフォン30から自分の氏名、住所を入力して送信すれば、S3によりYESの判断がなされてS4へ進み、乱数Rを生成してチャレンジデータとしてブラウザフォン30へ送信する処理がなされる。ユーザがVPの出生依頼を行なう場合には、ブラウザフォン30のUSBポート18にVP用IC端末19Vを差込んでおく。その状態で、VP管理サーバ9から乱数Rが送信されてくれば、その乱数をVP用IC端末19Vへ入力する。すると、後述するように、VP用IC端末19V内において入力された乱数RをRPの認証鍵KNを用いて暗号化する処理がなされ、その暗号結果がブラウザフォン30へ出力される。ブラウザフォン30では、その出力されてきた暗号化データであるレスポンスデータIをVP管理サーバ9へ送信する。すると、S5によりYESの判断がなされてS6へ進み、RPの認証鍵KNを用いて、受信したレスポンスデータIを復号化する処理すなわち $D_{KN}(I)$ を算出する処理がなされる。次にS7へ進み、S4により生成した乱数 $R = D_{KN}(I)$ であるか否かの判断がなされる。

## 【0111】

VPの出生依頼者が金融機関7のデータベース12に記憶されている正規のRPである場合には、 $R = D_{KN}(I)$ となるために、制御がS9へ進むが、データベース12に記憶されているRPに他人がなりすましてVPの出生依頼を行なった場合には、 $R = D_{KN}(I)$ とはならないために、制御がS8へ進み、アクセス拒絶の旨がブラウザフォン30へ送信されてS1へ戻る。

## 【0112】

一方、S7によりYESの判断がなされた場合には、S9へ進み、希望のコンビニエンスストアの入力があったか否かの判断がなされる。VPの出生依頼を行なったRPは、誕生してくるVPの住所となるコンビニエンスストアについて特に希望するコンビニエンスストアがあれば、ブラウザフォン30に入力してVP管理サーバ9へ送信する。その場合には、S9によりYESの判断がなされてS10へ進み、その入力されてきたコンビニエ

ンスストアの情報を記憶した後S12へ進む。一方、希望するコンビニエンスストアの入力がなかった場合にはS11へ進み、RPの住所に近いコンビニエンスストアを検索してそのコンビニエンスストアを記憶した後S12へ進む。

#### 【0113】

S12では、VPの氏名、VPの住所であるコンビニエンスストアの住所、VPのEメールアドレス等を決定する。次にS13へ進み、VPの公開鍵の送信要求をブラウザフォン30へ送信する。そして、S14へ進み、公開鍵KPの返信があったか否かの判断がなされ、あるまで待機する。VPの公開鍵の送信要求を受けたブラウザフォン30は、接続されているVP用IC端末19Vへ公開鍵出力要求を出力する。すると、後述するように、VP用IC端末19Vは、記憶しているVP用の公開鍵KPをブラウザフォン30へ出力する。ブラウザフォン30では、その出力されてきたVP用の公開鍵KPをVP管理サーバ9へ返信する。すると、S14よりYESの判断がなされてS15へ進み、RPに対応付けて、VPの氏名、住所、公開鍵KP、Eメールアドレスをデータベース12へ記憶させる処理がなされる。

#### 【0114】

次にS16へ進み、VPの電子証明書を作成してXMLストア50に登録する処理がなされる。この電子証明書は、金融機関7等の第三者機関においてRPとの対応関係が登録されている正規のVPであることを証明するものである。次にS17へ進み、RPに、VPの氏名、コンビニエンスストアの住所、コンビニエンスストアの名称、Eメールアドレス、電子証明書を記憶したIC端末19Iを郵送するための処理がなされる。次にS18へ進み、S12で決定された住所のコンビニエンスストアにVPの氏名、Eメールアドレス、当該金融機関7の名称を送信する処理がなされる。次にS19へ進み、正当機関である旨の証明処理がなされる。この正当機関である旨の証明処理は、前述したS1aと同じ処理である。次にS1へ戻る。

#### 【0115】

本発明でいう「匿名用の電子証明書」とは、ユーザと当該ユーザが用いる匿名（VP氏名）との対応関係を特定可能な情報を登録している守秘義務のある所定機関（金融機関7）により発行され、前記匿名を用いるユーザが当該所定機関に登録されているユーザであることを証明する証明書を含む概念である。よって、本人確認に用いる一般的なデジタルIDばかりでなく、前記所定機関が前記匿名を用いるユーザに対し当該ユーザは当該所定機関に登録されているユーザであることを証明する電子的な証明書をすべて含む概念である。たとえば、ユーザが用いる匿名とその匿名が前記所定機関に登録されているメッセージとに対し、前記所定機関によるデジタル署名が施されただけの、簡単な証明書を含む概念である。

#### 【0116】

S1によりNOの判断がなされた場合には図18(a)のS400へ進む。S400では、個人情報の登録処理が行なわれ、次にS401によりトラップ情報の登録処理が行なわれ、S402により個人情報の確認処理が行なわれ、S403により個人情報の照合、流通チェック処理が行なわれ、S404により個人情報の販売代行処理が行なわれ、S405によりメール転送、流通チェック処理が行なわれてS1へ戻る。ユーザから個人情報の提供を受けたサイト（業者）側では、提供してもらった個人情報が本当に正しい内容であるか否かを確認したいというニーズがある。そこで、金融機関7のVP管理サーバ9は、ユーザから個人情報を受付けたその個人情報が正しい個人情報かどうかをチェックし、正しい個人情報のみをデータベース12aに登録する。その処理をS400により行なう。

#### 【0117】

一方、ネットワーク上でVPの利用が盛んになった場合には、RPとVPとの両方の詳しい個人情報を収集した業者が、両個人情報をしらみつぶしにマッチングして、両個人情報が一致するRP氏名とVP氏名とを割出し、VPに対応するRPを予測してしまうという不都合が生ずる恐れがある。そこで、個人情報をデータベース12aに登録する場合に

は、勤務先名や所属部署名あるいは役職等のRPが特定されてしまうような個人情報を排除（または変更）して、登録する必要がある。そのような処理を、S400により行なう。

#### 【0118】

一方、個人情報主であるユーザは、自己の個人情報が正しい内容で流通しているか否かを監視し、間違っていれば正しい内容に修正したいというニーズがある。そこで、データベース12bに登録されている自己の個人情報の真偽をユーザがチェックできるように、S402により、個人情報の確認処理が行なわれる。

#### 【0119】

さらに、ユーザが自己の個人情報の公開範囲（流通範囲）を限定した上でその個人情報を業者側（サイト側）に提供した場合に、その公開範囲（流通範囲）が守られているか否かを監視したいというニーズがある。個人情報の提供を受けた業者側は、前述したようにその個人情報が正しい情報であるか否かを確認したいというニーズがある。そこで、サイト側（業者側）が所有している個人情報を正しい個人情報が登録されているデータベース12aの個人情報と照合できるようにする一方、その照合対象となった業者側所有の個人情報の流通許容範囲をチェックして正しく流通されているか否かを確認できるように、S403の処理が行なわれる。

#### 【0120】

ユーザは、個人情報を提供する見返りとして、何らかのサービスあるいは金銭を入手したいというニーズがある。そこで、S404により、個人情報の販売代行が行なわれる。図3に基づいて説明したように、トラップ型VPは、Eメールアドレスを金融機関7のトラップ型VP用として開設しているアドレスにしているため、そのトラップ型VPに宛てたEメールは金融機関7のトラップ型VP用に開設されたEメールアドレス宛に送られる。そこで、その送られてきたEメールを対応するVPのEメールアドレスに転送する必要がある。その処理を、S405により行なう。その際に、業者側から送られてくるEメールの宛名はトラップ型VPとなっているために、そのトラップ型VPに対応するサイト（業社）を割出し（図3参照）、その割出されたサイト（業社）からのEメールでなかった場合には当該トラップ型VPの個人情報の流通許容範囲内のサイト（業社）からのEメールか否かを確認し、流通チェックを行なうことも、S405により行なわれる。

#### 【0121】

図18（b）は、S400の個人情報の登録処理のサブルーチンプログラムを示すフローチャートである。この個人情報の登録処理は、ユーザがVPとして個人情報を登録する際の処理である。

#### 【0122】

乱数Rを受信したブラウザフォン30は、そのブラウザフォン30に接続されているVP用IC端末19Vに記憶されているVP用の秘密鍵を用いて乱数Rを1回暗号化してレスポンスデータIを生成する。そしてそのレスポンスデータIを金融機関7のVP用管理サーバ9へ送信する。

#### 【0123】

S410により、ユーザ側から個人情報の登録要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。登録要求があった場合にはS411へ進み、正当機関証明処理がなされる。次に制御がS412へ進み、VPの氏名の入力要求がなされ、S413により入力があったか否かの判断がなされる。入力があった場合には制御がS414へ進み、乱数Rを生成してチャレンジデータとして登録要求を行なったユーザ側に送信する処理がなされる。S415へ進み、ユーザ側からレスポンスデータIを受信したか否かの判断がなされ、受信するまで待機する。受信した段階でS416へ進み、VPの公開鍵KPをデータベース12aから検索して、受信したレスポンスデータIを公開鍵KPで暗号化したDKP（I）を生成する処理がなされる。

#### 【0124】

次に制御がS417へ進み、チャレンジデータRとDKP（I）が等しいか否かの判断が



なされる。等しくなければユーザの本人認証ができなかったこととなり S 4 2 2 へ進み、登録拒否の処理がなされる。S 4 1 7 により Y E S の判断がなされた場合には制御が S 4 1 8 へ進み、登録要求を出したユーザに対し登録を希望する個人情報の入力要求を出す処理がなされる。次に S 4 1 9 へ進み、入力があったか否かの判断がなされ、入力があるまで待機する。入力があった段階で制御が S 4 2 0 へ進み、登録対象の個人情報の真偽チェックを行なう。

#### 【0125】

この真偽チェックは、たとえば、XMLストア 50 にアクセスして該当するユーザの個人情報に登録されている場合にそれと照合チェックしたり、電子行政群 49 に含まれる市役所等にアクセスしてそこに登録されている個人情報と照合チェックしたりして行なわれる。このような機械検索による照合チェックだけでは不十分な場合には、金融機関 7 の調査員が裏取り調査を行なって真偽チェックを行なう。

#### 【0126】

次に制御が S 4 2 1 へ進み、真偽チェックの結果正しいか否かの判断がなされ、正しい場合には S 4 2 2 へ進み登録拒否の処理がなされる一方、正しい場合には S 4 2 3 へ進み、R P が特定される個人情報か否かの判断がなされる。登録しようとしている V P の個人情報の中に、たとえば勤務先名や所属部署名あるいは役職等の R P が特定されてしまうような個人情報が存在する場合に、それをそのまま登録してしまうと、その登録情報からの V P がどの R P に対応するかを第三者に予測されてしまう恐れがある。このデータベース 12 a に登録される個人情報は、S 4 0 3 や S 4 0 4 によりサイト側（業者側）が知り得る状態となる。その結果、サイト側（業者側）に、R P と V P との対応関係が予測される恐れが生ずる。

#### 【0127】

そこで、S 4 2 3 により、R P が特定される個人情報か否かの判断がなされ、予測される個人情報でなければ S 4 2 5 へ進むが、予測される恐れのある個人情報の場合には S 4 2 4 へ進み、その個人情報を加工する処理がなされた後 S 4 2 5 へ進む。たとえば、勤務先名が M E C であった場合には、それをたとえば「某大手電気メーカー」に加工したり、役職がたとえば専務であった場合には、たとえば「重役」に加工したりする。

#### 【0128】

S 4 2 5 では、個人情報に当該金融機関のデジタル署名を付してユーザ名別に登録する処理がなされる。その結果、図 4 に示すようなデータがデータベース 12 a に登録される。

#### 【0129】

図 19 は、S 4 0 1 に示されたトラップ情報の登録処理のサブルーチンプログラムを示すフローチャートである。S 4 3 0 により、正当機関証明処理がなされ、S 4 3 1 により、V P 氏名の入力要求がトラップ情報の登録依頼をしてきた V P に出される。次に S 4 3 2 へ進み、その登録依頼をしてきた V P が自己の V P 氏名を入力したか否かの判断がなされ、入力するまで S 4 3 1 の要求が出される。次に制御が S 4 3 3 へ進み、乱数 R を生成してチャレンジデータとして登録依頼者である V P に送信する処理がなされる。S 4 3 4 により、レスポンスデータ I を受信したか否かの判断がなされる。

#### 【0130】

送信されてきたチャレンジデータ R を受信した登録依頼者である V P がそのチャレンジデータ R を自己の秘密鍵で暗号化してレスポンスデータ I を生成し、金融機関 7 の V P 管理サーバ 9 へ送信する。すると、制御が S 4 3 5 へ進み、登録依頼をしてきた V P の公開鍵 K P をデータベース 12 a から検索し、受信したレスポンスデータ I をその公開鍵 K P で復号化する処理を行なう。そして S 4 3 6 により、チャレンジデータ  $R = D_{KP}(I)$  であるか否かの判断がなされ、イコールでない場合には認証の結果その V P が本人と確定できないということであり、S 4 3 7 により登録拒否の通知がその V P になされる。一方、S 4 3 6 により Y E S の判断がなされて認証の結果 V P が本人であることが確認できた場合には、制御が S 4 3 8 へ進み、トラップ情報の送信要求をその V P へ送信する処理がな

される。

#### 【0131】

VPから登録してもらいたいトラップ情報が送信されてきたか否かがS439によりなされ、送信されてくるまで待機する。送信されてきた段階で制御がS440へ進み、送信されてきたトラップ情報をデータベース12aに記憶させる処理がなされる。このトラップ情報は、登録依頼者であるVPに対応した記憶領域に記憶される。次に制御がS441へ進み、そのトラップ情報に対する電子署名を金融機関7が生成して、その電子証明書をXMLストア50へ登録する処理がなされる。その結果、図5に基づいて説明したように、XMLストア50のデータベース72に電子証明書が格納される。

#### 【0132】

この電子証明書は、XMLストア50に格納する代わりに登録依頼を行ってきたVPのIC端末19Vに格納してもよい。しかし、トラップ情報は、前述したように、そのVPがアクセスしたWebサイト毎またはVP（トラップ型VP）として登録してポイントカードを新規発行してもらった百貨店等の業社毎に異なり、その結果電子証明書もWebサイト毎（業社毎）に異なることとなり、多数の電子証明書をIC端末19Vに格納するとなると、記憶容量の問題が生ずる。ゆえに、本実施の形態では、その記憶容量の問題を克服するために、XMLストア50へ登録する。なお、IC端末19Vの記憶容量が非常に大きなものであれば、金融機関7が発行した電子証明書のすべてまたはその大半をこのIC端末19Vに記憶させてもよい。

#### 【0133】

図20は、S405に示されたメール転送、流通チェックのサブルーチンプログラムを示すフローチャートである。S514により、サイト（業者）からメールが送られてきたか否かの判断がなされる。図3等に基づいて説明したように、VPが、本名を用いてサイトにアクセスしたり業社にポイントカードを登録した場合にはVP自身のEメールアドレスをそのサイト側（業社側）に通知するが、トラップ型VP氏名を用いてサイト（業社）にアクセスした場合には、金融機関7のトラップ型VP用として開設されているEメールアドレスをそのサイト（業社）側に提供する。その結果、そのサイト（業社）からのEメールは、金融機関7のトラップ型VP用に開設されたEメールアドレスで送られてくることとなる。

#### 【0134】

金融機関7では、そのトラップ型VP用に開設したEメールアドレスに送信されてきたメールがある場合には、VP管理用サーバ9は、S514により、YESの判断を行なう。その結果、制御がS515へ進み、その送られてきたEメールに含まれている宛名に対応するサイト名（業者名）をデータベース12aから割出す処理を行なう。データベース12aは、図3に基づいて説明したように、VPの氏名とそのVPがアクセスしたサイト名（業社名）とが対応付けられて記憶されている。この対応関係を利用して、メールの宛名から対応するサイト名（業者名）を割出す処理がなされる。

#### 【0135】

次にS516により、割出されたサイト名（業社名）とEメールを送ったサイト名（業社名）とが一致するか否かの判断がなされる。本来なら一致する筈であるが、個人情報不正に流通された場合には、その不正流通された個人情報を不正入手したサイト（業社）がその個人情報主にEメールを送る場合がある。その場合には、割出されたサイト名（業社名）とメールを送ったサイト名（業社名）とが一致しない状態となる。

#### 【0136】

割出されたサイト名（業社名）とメールを送ったサイト名（業社名）とが一致しない場合に、即座に個人情報が不正流通されたとは断定できない。サイト（業社）側に個人情報を提供する際に、ある一定の流通許容範囲内においては流通させてもよいと個人情報主であるユーザから承諾を得ている場合がある。よって、S522に制御が進み、XMLストアの該当個人情報を検索して、ポリシーに定められている流通許容範囲内にEメール送信者が含まれるか否かチェックする処理がなされ、S523により、含まれると判断された



場合には制御がS517へ進むが、含まれないと判断された場合には制御がS519へ進む。

**【0137】**

S519では、Eメールを送ったサイト名（業社名）に対応させて個人情報の不正入手値を「1」加算更新する処理がなされ、S520により、S515によって割出されたサイト名（業社名）に対応させて個人情報の不正流出値を「1」加算更新する処理がなされる。次にS521により、個人情報の不正があった旨およびその詳細データを該当するユーザへ通知する処理がなされる。

**【0138】**

一方、個人情報不正流通されていないと判断された場合には制御がS517へ進み、Eメールの宛名に対応するユーザのメールアドレスを割出す処理がなされ、S518により、その割出されたアドレスにEメールを転送する処理がなされる。

**【0139】**

図21は、図2に示した認証用サーバ11の処理動作を示すフローチャートである。先ずS25により、RPから電子証明書の発行依頼があったか否かの判断がなされ、あるまで待機する。ユーザであるRPがブラウザフォン30からRPの電子証明書の発行依頼要求を認証用サーバ11へ送信すれば、制御がS26へ進み、RPの住所、氏名、公開鍵の送信要求をブラウザフォン30へ送信する処理がなされる。次にS27へ進み、ブラウザフォン30からRPの住所、氏名、公開鍵の返信があるか否かの判断がなされ、あるまで待機する。そして、返信があった段階で制御がS28へ進み、RPの電子証明書を作成してブラウザフォン30へ送信する処理がなされる。次にS29へ進み、RPの住所、氏名、公開鍵KPをデータベース12aに記憶する処理がなされてS25へ戻る。

**【0140】**

図22～図24は、図2の決済サーバ10の処理動作を示すフローチャートである。S35により、RPの銀行口座番号の作成依頼があったか否かの判断がなされ、ない場合にはS39へ進み、VPの銀行口座番号の作成依頼があったか否かの判断がなされ、ない場合にはS40へ進み、デビットカードの発行依頼があったか否かの判断がなされ、ない場合にはS41へ進み、決済依頼があったか否かの判断がなされ、ない場合にはS35へ戻る。

**【0141】**

このS35～S41のループの巡回途中で、ユーザが金融機関7へ出向き、RPの銀行口座の開設依頼を行なってRPの銀行口座番号の作成依頼が入力されれば、制御がS36へ進み、RPの住所、氏名等の入力要求がなされ、入力があれば制御がS38へ進み、RPの銀行口座を作成して、データベース12aに記憶するとともにRPに通知する処理がなされてS35へ戻る。

**【0142】**

ユーザが金融機関7へ出向き、VPの銀行口座の開設依頼を行なってVPの銀行口座番号の作成依頼要求が入力されれば、S42へ進み、VPの住所、氏名等、RPの住所、氏名等の入力要求がなされる。ユーザは、これら情報を手動でキーボードから入力するか、または、決済サーバ10にRP用IC端末19RやVP用IC端末19Vを接続してこれらデータを自動入力する。データが入力されれば、制御がS44へ進み、RPとVPの対応が適正であるか否かが、データベース12aを検索することにより確認される。

**【0143】**

RPとVPの対応が適正でない場合にはS51へ進み、対応が不適正である旨を報知してS35へ戻る。一方、RPとVPとの対応が適正な場合にはS45へ進み、VPの銀行口座を作成して、データベース12aに記憶するとともに、VPに対応するRPにその銀行口座を郵送する処理がなされた後S35へ戻る。

**【0144】**

ユーザが金融機関7へ出向き、デビットカードの発行依頼の依頼を行なってデビットカードの発行依頼の入力があれば、S40によりYESの判断がなされてS46へ進み、口

座番号と氏名と暗証番号の入力要求がなされる。ユーザがRP用のデビットカードの発行を要求する場合には、RPの銀行口座番号と氏名と暗証番号を入力する。一方、ユーザがVP用のデビットカードの発行要求を希望する場合には、VPの銀行口座番号とVPの氏名とVPの暗証番号とを入力する。これらのデータの入力は、RP用IC端末19RまたはVP用IC端末19Vを決済サーバ10へ接続して自動的に入力する。

**【0145】**

これらデータの入力が行なわれれば制御がS48へ進み、入力データをデータベース12aへ記憶するとともに、デビットカードを発行する処理がなされる。次にS49へ進み、発行されたデビットカードの記憶データをRP用IC端末またはVP用IC端末へ伝送する処理がなされてS35へ戻る。

**【0146】**

決済サーバ10に決済要求が送信されてくれば、S41によりYESの判断がなされてS50へ進み、決済処理がなされた後S35へ戻る。

**【0147】**

図23は、図22に示したS50の決済処理のサブルーチンプログラムを示すフローチャートである。決済要求には、銀行口座内の資金を一部RP用IC端末19RまたはVP用IC端末19Vに引落す引落し要求と、デビットカードを使用しての決済要求と、クレジットカードを使用して決済を行なった場合のクレジットカード発行会社からのクレジット使用金額の引落し要求とがある。まずS55よりIC端末19Rまたは19Vへの引落し要求があったか否かの判断がなされ、ない場合にはS57へ進み、デビットカードを使用しての決済要求があったか否かの判断がなされ、ない場合にはS58へ進み、クレジットカード発行会社からの引落し要求があったか否かの判断がなされ、ない場合にはS55へ進み、クレジットカード発行会社からの問合せ処理が行なわれた後、S59によりその他の処理がなされてこのサブルーチンプログラムが終了する。

**【0148】**

ユーザがブラウザフォン30等からRP用IC端末19RまたはVP用IC端末19Vへ資金の一部引落し要求を決済サーバ10へ送信した場合には、S55によりYESの判断がなされてS56へ進み、正当機関証明処理がなされた後S60へ進む。S60では、氏名の入力要求をブラウザフォン30等へ送信する処理がなされる。その要求を受けたブラウザフォン30では、接続されているIC端末19Rまたは19Vに対し氏名の出力要求を伝送する。すると、接続されているIC端末19Rまたは19Vから氏名がブラウザフォン30へ伝送され、その伝送されてきた氏名をブラウザフォン30が決済サーバ10へ伝送する。すると、S61によりYESの判断がなされてS62へ進み、乱数Rを生成してチャレンジデータとしてブラウザフォン30へ送信する処理がなされる。

**【0149】**

その乱数Rを受けたブラウザフォン30は、後述するように、接続されているIC端末19Rまたは19Vに対し乱数Rを伝送する。乱数Rを受取ったIC端末がRP用IC端末19Rの場合には、記憶している認証鍵KNを用いてRを暗号化してレスポンスデータIを生成し、それをブラウザフォン30へ出力する。ブラウザフォン30では、その出力されてきたレスポンスデータIを決済サーバ10へ送信する。一方、乱数Rを受取ったIC端末がVP用IC端末19Vの場合には、受取った乱数Rを記憶している公開鍵KPを用いて暗号化してレスポンスデータIを生成し、ブラウザフォン30へ出力する。ブラウザフォン30では、その出力されてきたレスポンスデータIを決済サーバ10へ送信する。

**【0150】**

レスポンスデータIが送信されてくれば、S63によりYESの判断がなされてS64へ進み、S60に応じて入力された氏名がRPのものであるか否かが判別され、RPの場合にはS65へ進み、RPの認証鍵KNをデータベース12から検索してその認証鍵KNを用いて受信したレスポンスデータIを復号化する処理すなわち $D_{KN}(I)$ を生成する処理がなされる。次にS66へ進み、 $R = D_{KN}(I)$ であるか否かの判断がなされる。IC

端末への引落し要求を行なったユーザがデータベース12に登録されている適正なユーザである場合には、 $R = D_{NK}(I)$  となるはずであるが、データベース12に登録されているユーザになりすまして銀行口座の資金の一部を引落しするという不正行為が行われた場合には、 $R$ と $D_{KN}(I)$ とが一致しない状態となる。その場合には制御がS79へ進み、不適正である旨をブラウザフォン30へ返信する処理がなされてサブルーチンプログラムが終了する。

**【0151】**

一方、 $R = D_{KN}(I)$  の場合には制御がS67へ進み、引落し額の入力要求をブラウザフォン30へ送信する処理がなされ、引落し額がブラウザフォン30から送信されてくれば、制御がS69へ進み、 $RP$ の口座から引落し額 $G$ を減算して $G$ をブラウザフォン30へ送信する処理がなされてサブルーチンプログラムが終了する。

**【0152】**

一方、ユーザがVPとしてVP用IC端末19Vへの引落しを行なう場合には、VPの本名を用いる。入力された氏名がVPの本名であった場合にはS64によりNOの判断がなされて制御が図24(a)のS85へ進む。S85では、VPの公開鍵KPをデータベース12から検索してその公開鍵KPを用いて受信したレスポンスデータIを復号化する処理すなわち $D_{KP}(I)$ を生成する処理がなされる。次にS86へ進み、 $R = D_{KP}(I)$ であるか否かの判断がなされる。引落し要求を行なっているものがデータベース12に登録されているVPになりすまして引落すという不正行為を行なっている場合には、S86によりNOの判断がなされてS79に進み、不適正である旨がブラウザフォン30へ返信されることとなる。一方、S86によりYESの判断がなされた場合にはS87へ進み、引落し額 $G$ の入力要求をブラウザフォン30へ送信する処理がなされ、ブラウザフォン30から引落し額 $G$ の送信があれば、S89へ進み、VPの銀行口座から $G$ を減算して $G$ をブラウザフォン30へ送信する処理がなされた後サブルーチンプログラムが終了する。

**【0153】**

ユーザがデビットカードを使用しての決済を行なうべくデビットカード使用操作を行なった場合には、デビットカード使用要求が決済サーバ10へ送信され、S57によりYESの判断がなされてS56へ進み、正当機関証明処理がなされる。次にS70へ進み、暗証番号とカード情報入力要求がユーザのブラウザフォン30へ送信される。デビットカードの暗証番号とデビットカード情報とがブラウザフォン30から決済サーバ10へ送信されてくれば制御がS72へ進み、その送信されてきたデータが適正であるか否かの判断がなされ、不適正であればS79へ進む。

**【0154】**

一方、適正である場合にはS73へ進み、使用額 $G$ の入力を待つ。ユーザが使用額 $G$ を入力してそれが決済サーバ10へ送信されてくれば制御がS74へ進み、該当する口座を検索して $G$ を減算するとともに $G$ をユーザのブラウザフォン30に送信する処理がなされる。

**【0155】**

ユーザがRPまたはVPの本名を用いて後述するようにクレジットカードによるSETを用いた決済を行なった場合には、クレジットカード発行会社4(図1参照)からクレジット支払金額の引落し要求が決済サーバ10へ送信される。その引落し要求が送信されてくればS58によりYESの判断がなされてS56の正当機関証明処理がなされた後S75へ進み、ユーザの氏名、口座番号の入力を待つ。クレジットカード発行会社4からユーザの氏名と口座番号とが送信されてくれば制御がS76へ進み、その入力されたデータが適正であるか否かをデータベース12を検索して判別する。不適正の場合にはS79へ進むが、適正な場合にはS77へ進み、引落し額 $G$ の入力を待機する。クレジットカード発行会社4から引落し額 $G$ すなわちクレジット支払額と手数料との合計金額が送信されてくれば制御がS78へ進み、口座から $G$ を減算してクレジットカード発行会社の口座 $G$ に加算する処理すなわち資金の移動処理がなされる。

**【0156】**

S 5 8 により N O の判断がなされた場合には S 5 5 4 によるクレジット発行会社 4 からの問合せ処理が行なわれた後 S 5 9 へ進み、その他の処理が行なわれる。

【0157】

図 2 4 (b) は、前述した S 1 a, S 1 9, S 5 6 に示された正当機関証明処理のサブルーチンプログラムを示すフローチャートである。まず S 9 0 により、当該機関の電子証明書を送信する処理がなされる。この電子証明書を受信した側においては、乱数 R を生成してその乱数 R を送信する。すると、S 9 1 により Y E S の判断がなされて S 9 2 へ進み、その受信した乱数 R を当該機関の秘密鍵 K S で暗号化する処理すなわち  $L = E_{KS}(R)$  を算出する処理がなされ、その算出された L を返信する処理がなされる。

【0158】

この L を受信した受信側においては、既に受信している電子証明書内の当該機関の公開鍵 K P を利用して L を復号化することにより R を得ることができる。その R と送信した R とがイコールであるか否かをチェックすることにより、正当機関であるか否かをチェックすることが可能となる。これについては後述する。

【0159】

図 2 5 は、S 5 5 4 に示されたクレジットカード会社からの問合せ処理のサブルーチンプログラムを示すフローチャートである。前述したように、V P がトラップ型 V P としてサイトにアクセスして電子ショッピング等を行なったりトラップ型 V P として登録している小売店等の業社で自動決済を行ってクレジット決済を行なった場合には、V P 本人のクレジット番号が用いられるのではなく、その V P 本人のクレジット番号を何回か秘密鍵で暗号化した暗号化クレジット番号が用いられることとなる。たとえば、図 3 に示すように、トラップ型 V P 氏名 E (B 1 3 P) としてサイト M P P にアクセスした V P は、電子ショッピング等を行なってクレジット決済をする際には、バーチャルクレジット番号 E (3 2 8 8) を用いる。V P は、クレジットカード発行会社 4 に対し 3 2 8 8 のクレジット番号は登録しているが、E (3 2 8 8) の暗号化クレジット番号までは登録していない。よって、E (3 2 8 8) のバーチャルクレジット番号がクレジット決済に伴ってクレジットカード発行会社 4 に送信されてきた場合には、クレジットカード発行会社 4 は、その E (3 2 8 8) のバーチャルクレジット番号を自社で検索して真偽を確かめることはできない。

【0160】

そこで、そのような場合に、クレジットカード発行会社は、金融機関 7 にそのバーチャルクレジット番号が正しいか否かの照会を行なってもらうのである。

【0161】

クレジットカード発行会社からの問合せがあれば制御は S 5 6 1 へ進み、S 5 6 1 ~ S 5 6 8 の前述したものと同様の認証処理が行なわれる。認証の結果本人が確認されれば S 5 6 7 により Y E S の判断がなされて S 5 6 9 へ進み、照会対象データの入力要求がクレジットカード発行会社へ送信される。この照会対象データとは、前述したバーチャルクレジット番号とトラップ型 V P 氏名とを含む。このトラップ型 V P 氏名をも入力されることにより、そのトラップ型 V P 氏名とバーチャルクレジット番号とが対応しているか否か等も照会できる。

【0162】

照会対象データがクレジットカード発行会社から送信されてくれば制御は S 5 7 1 へ進み、データベース 1 2 a を検索してその送信されてきた照会対象データと照合する処理がなされる。次に S 5 7 2 により、照合結果送られてきた照会対象データが適正であるか否かの判断がなされ、適正な場合に S 5 7 3 により、適正な旨をクレジットカード発行会社へ返信し、照合結果適正でない場合には S 5 7 4 により、不適正な旨がクレジットカード発行会社へ返信される。S 5 7 3 による適正な旨を返信する際には、S 5 7 0 により入力された照会対象データに対し適正な旨を表わす金融機関 7 側のデジタル署名を付し、そのデジタル署名付きデータが問合せをしたクレジットカード発行会社 4 へ返信されることとなる。

## 【0163】

図26は、図14のS95bに示されたブラウザフォン30の偽モード処理のサブルーチンプログラムを示すフローチャートである。SD1により、電源投入時であるか否かの判断がなされ、電源投入時でない場合にはSD2に進み、偽モード操作があったか否かの判断がなされ、ない場合にはSD3へ進み、偽モード解除操作があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。

## 【0164】

ブラウザフォン30の電源が投入されればSD1によりYESの判断がなされてSD4へ進み、現在のモードの種類をブラウザフォン30により表示する処理がなされる。ブラウザフォン30のモードは、偽モード、トラップモード、通常モードの3種類があり、現在どのモードになっているかが、SD4により表示される。次に制御がSD5へ進み、現在偽モードになっているか否かの判断がなされ、偽モードになっていない場合にはこの偽モード処理のサブルーチンプログラムが終了する。

## 【0165】

一方、偽モードになっている場合にはSD6へ進み、本人認証のためのパスワードを発信させて個人ユーザが所持している購入済物品に付されているRFIDタグに記憶させる処理がなされる。次にRFIDにOFFモード指令を発信する処理がSD7により行なわれる。これにより、購入済物品に付されているRFIDタグが、前述したようにOFFモード即ち記憶しているRFIDを発信しない発信停止モードとなる（SC6参照）。次にSD8へ進み、購入済物品に付されているRFIDタグに対しRFID送信指令を発信し、SD9により、そのRFIDタグからRFIDが発信されてそれを受信したか否かの判断がなされる。通常であれば、発信停止モードに切換わった後であるためにRFIDは発信されてくることがなく、SD10へ進み、RFID交換処理がなされる。一方、SD9によりRFIDを受信した旨の判断がなされた場合には、SD11へ進み、ブラウザフォン30によりエラー表示がなされる。

## 【0166】

個人ユーザがブラウザフォン30により偽モード操作を行なった場合には、SD2によりYESの判断がなされてSD12へ進み、ブラウザフォン30を偽モードに切換える処理がなされた後にSD6へ進む。一方、ブラウザフォン30により偽モード解除操作が行われた場合には、SD3によりYESの判断がなされて、SD13へ進み、ブラウザフォン30の偽モードを解除して通常モードにする処理がなされる。

## 【0167】

尚、この偽RFID発信機能を有するブラウザフォン30を有する個人ユーザは、前述のセキュリティ用のRFIDタグ1aを必ずしも所持する必要はない。ブラウザフォン30がセキュリティ用のRFIDタグ1aの代わりにしてくれるためである。

## 【0168】

図27は、SD10に示されたRFID交換処理のサブルーチンプログラムを示すフローチャートである。SE1により、交換希望電波をブラウザフォンから発信する処理がなされる。この交換希望電波は、最大20メートルの範囲までしか到達しない電波である。尚、この交換希望電波の到達距離を手動操作により変更設定地点例えば2メートル或いは5メートル等のように変更できるように構成してもよい。次にSE2に進み、交換エリア内即ち交換希望電波が到達する圏内から交換希望電波を受信したか否かの判断がなされる。受信した場合には、SE3へ進み、今日既に交換済みの相手（ブラウザフォン30）であるか否かの判断がなされ、既に交換済みのブラウザフォン30の場合には、交換処理を行なうことなくこのサブルーチンプログラムが終了する。交換済みの相手（ブラウザフォン30）であるか否かの判断を可能にするべく、前述の交換希望電波とともにブラウザフォン30を特定するためのIDコード等を送信してもよい。

## 【0169】

一方、今日まだRFIDの交換を行っていない相手（ブラウザフォン30）の場合には制御がSE4へ進み、偽RFIDを記憶しているか否かの判断がなされる。ブラウザフ

オン 30 の E E P R O M 194 に偽 R F I D を記憶しておれば、制御が S E 8 へ進み、その記憶している偽 R F I D (たとえば記憶中の 1 番新しい偽 R F I D) を交換相手のブラウザフォン 30 に発信すると共に、相手のブラウザフォン 30 から偽 R F I D を受信する処理がなされる。次に S E 9 へ進み、E E P R O M 194 に既に記憶している偽 R F I D を 1 つずつ古い記憶エリア側にシフトし、記憶上限を超えた 1 番古い偽 R F I D を消去する処理がなされる。次に S E 10 へ進み、1 番新しい記憶エリアに受信した偽 R F I D を記憶する処理がなされる。

#### 【0170】

一方、E E P R O M 194 に偽 R F I D を全く記憶していない場合には制御が S E 5 へ進み、個数決定用乱数 K R を生成して偽 R F I D の送信個数を決定する処理がなされる。次に S E 6 へ進み、その決定された個数だけの R F I D のコードを決定するための乱数 I D R を生成して偽 R F I D のコードを決定して発信する処理がなされる。次に S E 7 へ進み、相手からの偽 R F I D を受信して 1 番新しい記憶エリアに記憶する処理がなされる。

#### 【0171】

この R F I D 交換処理により、ブラウザフォン 30 を所持している個人ユーザが例えばすれ違う時に記憶している互いの偽 R F I D が交換されて記憶されることとなる。その結果、比較的同じ場所を移動する個人ユーザ同士で偽 R F I D を交換しあって互いの共通偽 R F I D として記憶して、R F I D 送信要求があった場合にはその共通偽 R F I D を発信することができる状態となり、比較的同じ場所を移動する個人ユーザ同士で前述の異人物同一識別子発信現象を生じさせることができ、悪意のプライバシー侵害者を有効に攪乱することができる。

#### 【0172】

図 28 は、図 14 の S 95 c に示されたトラップモードを処理のサブルーチンプログラムを示すフローチャートである。S F 1 により、トラップモード操作があったか否かの判断がなされ、ない場合には S F 2 へ進み、トラップモード解除操作があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。個人ユーザが自己のブラウザフォン 30 を操作してトラップモード操作を行なった場合には、S F 1 により Y E S の判断がなされて S F 3 へ進み、ブラウザフォン 30 はトラップモードに切換わる。

#### 【0173】

次に S F 4 へ進み、当該ユーザが所持している購入済物品に付されている R F I D に対しパスワードを発信する処理がなされる。次に S F 5 へ進み、O F F モード指令がその R F I D へ発信される。次に S F 6 により、R F I D 送信指令が発信され、S A F 7 により、R F I D の受信があったか否かの判断がなされる。S F 5 により既に O F F モード指令が発信されているために、当該ユーザが所持する購入済物品に付されている R F I D タグが発信されることは通常あり得ない。よって、通常は、S F 7 により N O の判断がなされて、制御が S F 7 a へ進む。S F 7 a では、業社選択指定操作があるか否かの判断がなされる。ない場合には S F 8 へ進み、個人ユーザが自己のブラウザフォン 30 により罍を仕掛ける相手業社を選択指定した場合には、制御が S F 7 b へ進み、選択指定された業者を記憶する処理がなされた後に S F 8 へ進む。

#### 【0174】

次に、S F 8 により、トラップモード切換え完了の表示がブラウザフォン 30 によりなされる。一方、S F 7 により R F I D の受信があったと判断された場合には S F 9 へ進み、ブラウザフォン 30 によりエラー表示がなされる。

#### 【0175】

次に、個人ユーザが自己のブラウザフォン 30 を操作してトラップモード解除操作を行なった場合には、S F 2 により Y E S の判断がなされて S F 10 へ進み、当該ブラウザフォン 30 のトラップモードが解除される。

#### 【0176】

図 29 は、図 14 の S 95 d に示された R F I D 発信処理のサブルーチンプログラムを示すフローチャートである。S G 1 により、R F I D 送信指令を受信したか否かの判断が



なされる。受信していなければこのサブルーチンプログラムが終了する。一方、タグリーダーからRFID送信指令が発信されれば、ブラウザフォン30がそれを受信してSG1によりYESの判断がなされ、SG2により、受信した旨の報知がブラウザフォン30によりなされる。この報知は、具体的には、ブラウザフォン30から受信音を発生させると共にRFID送信要求の電波を受信した旨の表示を液晶表示画面に示す。

**【0177】**

次に制御がSG3へ進み、偽モードになっているか否かの判断がなされる。偽モードになっていない場合にはSG4へ進み、トラップモードになっているか否かの判断がなされる。トラップモードになっていない場合即ち通常モードの場合にはこのサブルーチンプログラムが終了する。従って、通常モードの場合には、RFID送信指令を受信したとしても、何らRFIDを発信する処理が行なわれない。

**【0178】**

ブラウザフォン30は偽モードになっている場合にはSG3によりYESの判断がなされて制御がSG3aへ進み、前回のRFIDの発信から5秒経過しているか否かの判断がなされる。5秒経過していない場合にはSG3bへ進み、前回発信したRFIDと同じコードのRFIDを発信する処理がなされる。これは、タグリーダーの読取り信頼性を向上させるべくタグリーダーから短期間の間に連続して複数回RFID送信要求が送られてくることを想定したものであり、その場合毎回ランダムに生成された偽RFIDを発信したのでは、適正なRFIDとして読取ってくれない不都合が生じる。そこで、前回のRFID発信から5秒経過していない時には、前回と同じコードのRFIDを発信するようにし、偽RFIDであることが見破られる不都合を防止できるようにしている。また、タグリーダーの読取り信頼性を向上させる目的ではなく、受信したRFIDが本物のRFIDであるかまたは偽物のRFIDであるかを見極めるために連続して複数回RFID送信要求を発信するタグリーダーが設置される可能性も予測される。そのようなタイプのタグリーダーが設置されたとしても、所定期間内（例えば5秒間）の範囲内で再度RFID発信要求が行われてくれば、前回と同じコードのRFIDを送り返すために、偽RFIDであることが見破られる不都合を防止できる。この場合、第1回目の偽RFIDを送信した後一旦電源用電波が停止され、その後（例えば5秒後）再度電源用電波が発信されてRFID発信要求が行われたとしても、コンデンサ110からの供給電力によりRFIDタグ1aが作動中であるため、前回と同じ偽RFIDを再発信することができる。

**【0179】**

前回のRFIDの発信から5秒経過している場合にはSG3aによりYESの判断がなされてSG5へ進み、偽RFIDがEEPROM194に記憶されているか否かの判断がなされる。記憶されている場合には、SG9へ進み、その記憶している偽RFIDの内前回発信したRFIDの次の順番のRFIDを発信する処理がなされる。一方、偽RFIDの記憶がない場合には、SG6へ進み、個数決定用乱数KRを生成してRFIDの送信個数を決定する処理がなされ、SG7により、その決定された個数だけのRFIDのコードを決定するための乱数IDRを生成して偽RFIDの各コードを決定して発信する処理がなされる。そして、SG8により、その決定された偽RFIDをそれぞれEEPROM194に記憶させる処理がなされる。

**【0180】**

ブラウザフォン30がトラップモードとなっている場合には、SG4により、YESの判断がなされてSG10へ進み、業社の店名を受信しているか否かの判断がなされる。後述する自動決済処理等の場合には、販売業者の店名信号を受信する（SH2参照）。業社の店名を受信しておれば、制御がSG11へ進み、受信した業社に対応するトラップ型RFIDがVP用IC端末19Vに記憶されているか否かの判断がなされる（図8、図9参照）。記憶されている場合にはSG12へ進み、その受信し業社に対応するトラップ型RFIDを発信する処理がなされる。一方、SG10またはSG12によりNOの判断がなされた場合には制御がSG13へ進み、図28のSF7bにより予め選択指定されている業者に対応するRFIDをVP用IC端末19VのEEPROM26から読出して（図8

、図9参照)、そのトラップ型RFIDを発信する処理がなされる。例えば、個人ユーザがポイントカードの発行を行っていないスーパーマーケット等の業社内を歩いたりその業社内で購入商品を自動決済した場合等においてその業社側からRFID送信要求が発信された場合には、SF7bにより予め選択指定されている業者に対応するトラップ型RFIDが発信されることとなる。例えば、個人ユーザがMTTの業社を選択操作してSF7bによりその選択指定された業者MTTをブラウザフォン30に記憶させた場合において、ポイントカードを新規発行していないすなわちVPを登録していないスーパーマーケット(RIFに)においてRFID送信要求が出された場合には、ブラウザフォン30からMTTに対応するトラップ型RFIDであるmttが発信されることとなる。そのトラップ型RFIDであるmttを発信した後、スーパーマーケットRIFがトラップ型VPであるE(B13P)宛にダイレクトメールあるいはEメールが送信されてきた場合には(図9参照)、業社MTTに登録されているトラップ型VPの個人情報E(B13P)、Eメールアドレス△△△△△等が、業社MTTからスーパーマーケットRIFに不正に横流しことが分かる。このように、トラップ型RFIDを発信することにより、後日送られてきた電子メールやダイレクトメールの宛名と送り主とをチェックすることにより、個人情報が不正に横流しされたか否かをチェックすることが可能となる。

#### 【0181】

図30は、個人ユーザが百貨店等の業社において商品を購入した後自動決済を行なう場合の決済用ゲートの通過状態を示す説明図である。百貨店(業社)206により個人ユーザ202が商品を購入して手提げ袋203に詰め込み、決済用の通過ゲート206を通過して購入商品の決済を行なう。購入商品には、それぞれにRFIDタグが付されており、通過ゲート206に設けられているタグリーダライタ201との間で交信を行なう。また、個人ユーザ202はブラウザフォン30を所持している。

#### 【0182】

百貨店(業社)206には、決済サーバ204とデータベース205とが設置されている。決済サーバ204は、通過ゲート206に設けられているタグリーダライタ201と電氣的に接続されている。タグリーダライタ201は、通過ゲート206を通過する際に個人ユーザ202の所持しているブラウザフォン30および個人ユーザ202の手提げ袋203内に収納されている購入商品に付されているRFIDタグと交信を行ない、決済に必要なデータを決済サーバ204へ送信する。決済サーバ204に接続されているデータベース205には、顧客データが記憶されている。具体的には、顧客名E(B13P)、E(NPXA)…と、それら各顧客名に対応するポイント数、住所、Eメールアドレスが記憶されている。住所は、トラップ型VPであるE(B13P)のコンビニエンスストアの住所□×○、E(NPXA)のコンビニエンスストアの住所である△○○(図3参照)であり、Eメールアドレスは、トラップ型VPの場合には金融機関7に開設しているトラップ型VP用のEメールアドレスである△△△△△となっている(図3参照)。なお、購入商品に付されているRFIDタグは、決済用ゲートを通過して決済が完了し時点でタグリーダライタ201からの所定の信号(たとえば決済完了信号)を受信した初めてRFID発信停止状態にすることが可能となる。したがって、決済完了前においては、SD7、SF5等に従ってブラウザフォン30からOFFモード指令が発信されたとしてもRFID発信停止状態にはならない。

#### 【0183】

図31は、図14のS100に示された自動決済処理のサブルーチンプログラムを示すフローチャートである。SH1により、自動決済開始信号を受信したか否かの判断がなされる。個人ユーザ202が通過ゲート206を通過する際にタグリーダライタ201から自動決済開始信号がブラウザフォン30に送信されて来れば、SH1によりYESの判断がなされてSH2へ進み、販売業社である百貨店206の店名信号を受信したか否かの判断がなされ、受信するまで待機する。タグリーダライタ201から店名信号がブラウザフォン30へ送信されて来れば、SH3へ進み、送信されてきた店名(業社名)に対応するトラップ型RFIDがVP用IC端末19Vに既に記憶されているか否かの判断がなされ



る。既に記憶されている場合にはSH5へ進み、まだ記憶されていない場合にはSH4へ進み、送信されて来た店名(業社名)に対応させて新しいトラップ型RFIDを生成してVP用IC端末19VをEEPROM26に記憶させる処理がなされる。

#### 【0184】

次にSH5へ進み、送信されてきた店名の業社がポイントカードを発行して登録している業社であるか否かの判断がなされる。ポイントカードの登録がなされていない場合にはSH14へ進むが、ポイントカードの発行がなされている業社の場合にはSH6へ進み、デビット決済、クレジットカード決済の両方が可能な旨をブラウザフォン30により表示する処理がなされる。

#### 【0185】

SH1～SH6の処理の間に、タグリーダー201は手提げ袋203に収納されている各購入商品に付されているRFIDタグと交信してそのRFIDタグから送信されてきた各RFIDを決済サーバ204へ送信する。決済サーバ204は、その送信されてきた各RFIDに対応する商品価格を割出してその合計を算出してタグリーダー201へ送信する。タグリーダー201は、その合計金額を個人ユーザ203のブラウザフォン30へ送信する。

#### 【0186】

次に制御はSH7へ進み、払出金額を受信する処理がなされる。タグリーダー201から合計金額(払出金額)がブラウザフォン30へ送信されてくることにより、この支払い金額の受信処理が行なわれる。次にSH8へ進み、決済処理の入力操作があったか否かの判断がなされる。個人ユーザ202がブラウザフォン30により決済処理を入力する。決済の種類は、前述したデビットカード決済とクレジットカード決済とリロード金額決済とがある。リロード金額決済とは、個人ユーザ202の銀行口座の残額から一部ブラウザフォン30に引き落としてブラウザフォン30にリロードした金額を用いて決済を行なうものである。次にSH9へ進み、SH7により受信された支払金額をブラウザフォン30により表示する処理がなされる。次にSH10へ進み、その支払い金額に同意して決済を行なうためのOK操作があったか否かの判断がなされる。OK操作がない場合にはSH11へ進み、決済をキャンセルするキャンセル操作があったか否かの判断がなされ、ない場合にはSH10へ戻る。このSH10、SH11のループの巡回途中で、顧客202がブラウザフォン30を操作してOK操作を入力すれば制御がSH13へ進む。一方、個人ユーザ202がキャンセル操作を行なえばSH12へ進み、ブラウザフォン30からタグリーダー201へキャンセル信号が発信され、商品の購入をキャンセルする意思表示が送信される。

#### 【0187】

SH13では、SG8により入力された決済の種類がリロード金額決済であるか否かの判断がなされる。リロード金額決済の場合にはSH14へ進み、SH7により受信した支払金額をブラウザフォン30にリロードされているリロード金額との大小関係を判別し、支払金額以上のリロード金額があるか否かの判断がなされる。支払金額以上のリロード金額がある場合にはSH15によりOK信号がブラウザフォン30からタグリーダー201へ送信され、その信号が決済サーバ204へ送信される。次にSH16により、VP用決済処理がなされる。このVP用決済処理は、図53～図55にその詳細が示されている。SH16の場合にはリロード金額決済を行なうために、図55のS249によりYESの判断がなされてS250～S252bの処理が行なわれることとなる。

#### 【0188】

次にSH17により、ポイントカード加算処理が行なわれる。このポイントカード加算処理は、購入商品の合計金額に対応するポイント数をポイントカードに加算するための処理であり、図32(a)に示されている。

#### 【0189】

一方、SH14によりNOの判断がなされた場合には、SH18へ進み、キャンセル信号をブラウザフォン30からタグリーダー201へ送信する処理がなされ、その信号

が決済サーバ204へ送信される。次にSH19へ進み、残額不足である旨の表示がブラウザフォン30により行なわれる。

#### 【0190】

なお、決済相手の業社がポイントカードを登録していない業社の場合にはSH5によりNOの判断がなされてSH14～SH19のリロード決済の処理が行なわれることとなり、クレジット決済やデビット決済は行なわれない。これは、ポイントカードを登録していない業社の場合には個人ユーザ202のVP情報をその業社に登録していないために、VPとしてクレジット決済やデビット決済を行なうことが不可能なためである。

#### 【0191】

SH13によりNOの判断がなされた場合にはSH20へ進み、入力された決済処理がクレジット決済であるか否かの判断がなされる。クレジット決済の場合にはSH22に進み、OK信号がブラウザフォン30からタグリーダライタ201へ送信され、その信号が決済サーバ204へ送信される。次に、SH23へ進み、VP用決済処理が行われる。このSH23のVP用決済処理は、クレジット決済であるために、図55のS238によりYESの判断がなされてS237～S248のクレジット決済処理が行なわれることとなる。

#### 【0192】

入力された決済処理がデビット決済の場合にはSH20によりNOの判断がなされてSH21へ進み、デビット決済要求信号をブラウザフォン30がタグリーダライタ201へ送信し、その信号が決済サーバ204へ送信される。決済サーバ204は、データベース200を検索して決済相手の顧客名に対応するバーチャル口座番号例えばE(2503)を割出し(図30参照)、そのバーチャル口座番号内に残額がどの程度あるかを金融機関7に問い合わせる。そして、残額が支払金額以上の場合には、OK信号をタグリーダライタ201を介してブラウザフォン30へ送信する。一方、残額が支払金額未満であった場合には、NG信号をタグリーダライタ201を介してブラウザフォン30へ送信する。

#### 【0193】

ブラウザフォン30では、SH24により、OK信号を受信したか否かの判断がなされ、未だに受信していない場合にはSH26によりNG信号を受信したか否かの判断がなされ、未だに受信していない場合にはSH24へ戻る。

#### 【0194】

SH24、SH26のループの巡回途中で、タグリーダライタ201からOK信号がブラウザフォン30へ送信されてくれば、制御がSH25へ進み、VP用決済処理がなされる。この場合には、デビット決済であるために、図54(b)のS220によりYESの判断がなされてS235～S234のデビット決済処理が行なわれることとなる。

#### 【0195】

タグリーダライタ201からNG信号がブラウザフォン30へ送信されてくれば、SH26によりYESの判断がなされてSH27へ進み、NG表示がブラウザフォン30により行なわれる。

#### 【0196】

図32(a)は、SH17に示されたポイントカード加算処理のサブルーチンプログラムを示すフローチャートである。SI1により、該当するVP情報を発信する処理が行なわれる。これは、決済相手の業社に登録されているVPをVP用IC端末19VのEEPROM26から検索し、その検索されたVP氏名等の情報(例えばE(B13P))をタグリーダライタ201へ送信する。タグリーダライタ201は、その受信したVP情報を決済サーバ204へ送信する。決済サーバ204は、受信したVP氏名に基づいてデータベース205を検索し(図30参照)、例えば受信した顧客名がE(B13P)の場合には、現在のポイント数19018を割出して、その現在のポイント数に対し、購入商品の合計金額に対応したポイント数を加算する処理を行なう。そしてその加算ポイント数を決済サーバ204がタグリーダライタ201を介してブラウザフォン30へ送信する。

#### 【0197】

ブラウザフォン30では、S I 2によりポイント受信したか否かの判断がなされ、あるまで待機する。そして、タグリーダー201から加算ポイント数を受信すれば、制御がS I 3へ進み、該当する業社(決済相手の業社)に対応させてVP用IC端末19VのEEPROM26に記憶させる処理が行なわれる。

#### 【0198】

図23(b)は、百貨店等の業社206においてポイントカードを新規発行して登録してもらう際のブラウザフォン30の処理動作を示すフローチャートである。S J 1により、個人ユーザ202がポイントカード登録操作をブラウザフォン30により行なったか否かの判断がなされ、行なった場合にはS J 2へ進み、金融機関7に既に登録されているトラップ型VPであって未だポイントカード登録に用いられていないトラップ型VPはVP用IC端末19VのEEPROM26に記憶されているか否かの判断がなされる。判断の答えがNOの場合にはS J 3へ進み、トラップ型VPがない旨の表示がブラウザフォン30により行なわれる。その際には、個人ユーザ202は、金融機関7に対して、新たなトラップ型VPを生成して登録してもらうための処理を行なう。新たなトラップ型VPの生成要求があった場合には、金融機関7のVP管理サーバ9は、図37または図40(b)のトラップ型VP処理を行なって新たなトラップ型VPを生成して登録する処理を行なう。

#### 【0199】

一方、S J 2により常に登録されているトラップ型VPであってポイントカードの登録にまだ用いられていないトラップ型VPの記憶があると判断された場合には、S J 4へ進み、そのトラップ型VPの中から1つ選択してその住所、氏名等の必要な情報をブラウザフォン30からタグリーダー201を介して決済サーバ204へ送信する処理が行なわれる。決済サーバ204は、受信したトラップ型VP情報に基づいてポイントカードの新規登録を行なっているか否かの判断を行ない、その判断結果をタグリーダー201を介してブラウザフォン30へ返信する。

#### 【0200】

ブラウザフォン30では、S J 5により、OK信号を受信したか否かの判断を行ない、未だ受信していない場合にはS J 6によりNG信号を受信したか否かの判断を行ない、未だ受信していない場合にはS J 5へ戻る。このS J 5、S J 6のループの巡回途中で、決済サーバ204の判断結果としてOK信号を受信すれば、S J 5によりYESの判断がなされてS J 7へ進み、ポイントカードの登録相手である業社名を受信したか否かの判断がなされる。決済サーバ204は、OK信号を送信した後、当店の業社名をタグリーダー201を介してブラウザフォン30へ送信する。すると、S J 7によりYESの判断がなされてS J 8へ進み、その受信した業社名に対応させてトラップ型VPをVP用IC端末19VのEEPROM26へ記憶させる処理がなされる。

#### 【0201】

一方、決済サーバ204からの判断結果がNGであった場合には、S J 6によりYESの判断がなされてS J 9へ進み、NG表示がブラウザフォン30により行なわれる。

#### 【0202】

図33は、販売業社206の決済サーバ204の決済処理を示すフローチャートである。S K 1により、自動決済の開始であるか否かの判断がなされ、自動決済の開始でない場合にはS K 2に進み、ポイントカードの新規登録要求であるか否かの判断がなされ、新規登録要求でない場合にはS K 3へ進み、その他の処理が行なわれてS K 1へ戻る。

#### 【0203】

個人ユーザ202が決済のために通過ゲート206を通過した場合には、S K 1によりYESの判断がなされてS K 4へ進み、店名(業社名)の信号を決済サーバ204がタグリーダー201を介してブラウザフォン30へ送信する指令処理を行なう。次にS K 5へ進み、RFID送信要求の信号をタグリーダー201に発信させるための指令処理を行なう。次にS K 6へ進み、RFIDを受信したか否かの判断がなされ、受信するまで待機する。手提げ袋203に収納されている各購入商品に付されているRFIDタグか

ら発信された各RFIDがタグリーダー201に読取られてその信号が決済サーバ204へ送信される。すると、SK6によりYESの判断がなされてSK7へ進み、受信した各RFIDの内当店の販売商品として登録されているRFIDを検索する処理がなされる。百貨店(業社)206のデータベース205には、図31に示した顧客データばかりでなく、販売商品の各RFIDとそれに対応させた商品価格データが記憶されている。決済サーバ204は、データベース205を検索して、データベース205に登録されているRFID中に送信されてきたRFIDと一致するものであるか否かを判別し、一致するものを検索する。そしてSK8により、その一致するRFIDの商品価格の合計を算出する処理がなされる。次に、SK9へ進み、その算出した合計金額を支払い金額としてタグリーダー201を介してブラウザフォン30へ送信する処理が行なわれる。

#### 【0204】

次にSK10へ進み、ブラウザフォン30からOK信号を受信したか否かの判断がなされ、またSK11により、ブラウザフォン30からキャンセル信号を受信したか否かの判断がなされる。このSK10、SK11のループの巡回途中で、ブラウザフォン30からOK信号が送信されてくればSK12により決済処理を行なう。この決済処理は、図53～図55のブラウザフォン30側の決済処理動作に対応した販売業者側の決済サーバ204の処理動作である。次にSK13へ進み、販売された商品のRFIDをデータベース205の登録から抹消する処理がなされる。次にSK14へ進み、販売商品の合計金額に対応する加算ポイント数を算出する処理がなされる。

#### 【0205】

SK15へ進み、VP情報を受信したか否かの判断がなされ、受信するまで待機する。SI1に従ってブラウザフォン30から該当するVP情報が送信されて来れば、制御がSK16へ進み、加算ポイント数をタグリーダー201からブラウザフォン30へ送信する処理がなされる。次にSK17へ進み、受信したVPに対応するポイントデータをデータベース205から割出し(図30参照)、その割出されたポイント数に対し加算ポイント数を加算更新する処理がなされてSK1へ戻る。

#### 【0206】

次に、ポイントカードの新規登録要求があった場合にはSK2によりYESの判断がなされてSK21へ進み、VPを受信したか否かの判断がなされ、受信するまで待機する。SJ4に従ってブラウザフォン30からトラップ型VP情報が送信されてくれば、制御がSK22へ進み、金融機関7のVP管理サーバ9に適正に登録されているVPであるか否かの問合せ処理がなされる。VP管理サーバ9では、データベース12aに適正に登録されているVPであるか否かをチェックし、そのチェック結果を販売業者206の決済サーバ204へ返信する。決済サーバ204では、返信されてきたチェック結果が適正であるか否かSK23により判定し、適正でない場合にはSK24によりNGをタグリーダー201を介してブラウザフォン30へ返信する処理がなされる。一方、適正である場合にはSK18へ進み、OK信号をタグリーダー201を介してブラウザフォン30へ返信する処理がなされる。

#### 【0207】

SK19へ進み、店名(業社名)をタグリーダー201を介してブラウザフォン30へ送信する処理がなされ、SK22により、ポイント対象顧客としてVPをデータベース205に新規登録する処理がなされる(図30参照)。

#### 【0208】

次に、VP用IC端末19Vの制御動作を図34に基づいて説明する。VP用IC端末19Vは、S253により、暗証番号チェック処理を行なう。次にS254へ進み、トラップ型RFID処理を行なう。次にS255へ進み、本人証明処理を行なう。次にS256へ進み、データ入力処理を行なう。次にS257へ進み、ユーザエージェント動作処理を行なう。次にS258へ進み、リロード金額の使用処理を行なう。次にS259へ進み、署名処理を行なう。次にS615により、トラップ型VP処理がなされる。この処理は、図37に基づいて後述する。

## 【0209】

図35(a)は、S253に示された暗証番号チェック処理のサブルーチンプログラムを示すフローチャートである。S268により、暗証番号が入力されたか否かの判断がなされ、入力されていない場合にはこのままサブルーチンプログラムが終了する。一方、暗証番号が入力されれば、S269へ進み、入力された暗証番号を記憶している暗証番号と照合する処理がなされる。次にS270へ進み、照合の結果一致するか否かの判断がなされ、一致しない場合にはS271へ進み、不適正な旨をブラウザフォン30へ送信する処理がなされる。一方、一致する場合にはS272へ進み、適正な旨の返信を行なう。

## 【0210】

図35(b)は、S254に示されたトラップ型RFID処理(VP用)のサブルーチンプログラムを示すフローチャートである。S273により、業社名の入力があるか否かの判断がなされる。ブラウザフォン30はVP用IC端末19Vにトラップ型RFIDに対応する業社名(店名)を入力する(SG11、SG13、SH3)。入力があればS274へ進み、入力された業社名に対応するトラップ型RFIDの読出し要求か否かが判断される。SG11、SG13にしたがった要求の場合にはS274によりYESの判断がなされ、S275により、EEPROM26に記憶されているトラップ型RFIDの中から入力された業社名に対応するトラップ型RFIDを検索する処理がなされる。検索の結果対応するトラップ型RFIDが記憶されているか否かがS276により判断される。記憶がある場合にはその対応するトラップ型RFIDをブラウザフォン30へ出力する処理がS277によりなされる。一方、S276により対応するトラップ型RFIDの記憶がないと判断された場合には、ブラウザフォン30へ出力する処理がなされる。

## 【0211】

ブラウザフォン30は、記憶がない旨の信号を受信した場合には、SH3によりNOの判断を行ない、SH4により、業社名に対応させてトラップ型RFIDを記憶させる指令をVP用IC端末19Vへ出力する。それを受けたVP用IC端末19Vは、S273によりYES S274によりNOの判断を行い、S278により、新たなトラップ型RFIDを生成して、業社名に対応させてEEPROM26に記憶する処理を行なう。

## 【0212】

図35(c)は、S255に示された本人証明処理(VP用)のサブルーチンプログラムを示すフローチャートである。S280により、乱数Rの入力があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。乱数Rの入力があった場合にS281へ進み、VP出生依頼時であるか否かの判断がなされる。VP出生依頼時の場合には、S6、S151で説明したように、RPの認証鍵KNを用いてRPが正当な本人であることを証明する必要がある。そのために、VP出生依頼時の場合にはS283進み、入力された乱数RをRPの認証鍵KNで暗号化してIを生成する処理すなわち $I = E_{KN}(R)$ の算出処理を行なう。そして、S284により、その算出されたIをブラウザフォン30へ出力する処理がなされる。

## 【0213】

一方、VP出生依頼時でない場合には、S281によりNOの判断がなされてS282へ進み、VPは正当な本人であることを証明するべく、VPの秘密鍵KSを用いて入力された乱数Rを暗号化してIを算出する処理、すなわち、 $I = E_{KS}(R)$ を算出する処理を行なう。そしてS248により、その算出されたIをブラウザフォン30へ出力する処理がなされる。

## 【0214】

図36(a)は、S256、S263に示されたデータ入力処理のサブルーチンプログラムを示すフローチャートである。S293により、データ入力があったか否かの判断がなされる。入力されるデータとしては、前述したように、VP管理サーバ9によって誕生したVPに関するデータが記録されているCD-ROMの記録データ、ユーザエージェントの知識データ(S179、S189参照)、引落し額G(S181、S191参照)等がある。これらのデータが入力されれば、制御がS294へ進み、入力データに対応する

記憶領域に入力データを記憶させる処理がなされる。

【0215】

図36(b)は、S257、S264に示されたユーザエージェント動作処理のサブルーチンプログラムを示すフローチャートである。S295により、公開鍵出力要求があったか否かの判断がなされる。公開鍵の出力要求があった場合には、S298に進み、記憶している公開鍵KPを出力する処理がなされる。S295によりNOの判断がなされた場合にS296へ進み、デビットカード情報の出力要求があったか否かの判断がなされる。あった場合にはS299へ進み、記憶しているデビットカード情報を出力する処理がなされる。

【0216】

S296によりNOの判断がなされた場合にはS297へ進み、クレジットカード情報の出力要求があったか否かの判断がなされる。あった場合にはS300へ進み、記憶しているクレジットカード情報を出力する処理がなされる。次にS301へ進み、その他の動作処理が行なわれる。このその他の動作処理は、図30に基づいて後述する。

【0217】

図36(c)は、S258、S265に示されたリロード金額の使用処理のサブルーチンプログラムを示すフローチャートである。S302により、引落とし額Gの引落とし要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。あった場合には、S303へ進み、記憶しているリロード金額がGを減算する処理がなされ、S304へ進み、引落とし完了信号を返信する処理がなされる。

【0218】

図36(d)は、S259により示されたVP署名処理のサブルーチンプログラムを示すフローチャートである。S999により、メッセージダイジェストMDとVP氏名との入力ブラウザフォン30からあったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。

【0219】

MDとVP氏名との入力があった場合には制御がS998へ進み、その入力されたVP氏名から秘密鍵(KS)を生成する処理がなされる。具体的には、VP用IC端末19Vは、入力されたVP氏名に基づいてトラップ型RFIDデータ記憶領域を検索してその入力されたVP氏名が本名B13P(図9参照)を何回暗号化したものであるかを割出す。その割出された暗号化回数だけVPの秘密鍵をVPの秘密鍵で暗号化して秘密鍵(KS)を生成する。

【0220】

次に制御がS997へ進み、その秘密鍵(KS)を用いてメッセージダイジェストMDを復号化して二重署名を生成する処理がなされる。次に制御がS998へ進み、その二重署名D<sub>(KS)</sub>(MD)をブラウザフォン30へ出力する処理がなされる。

【0221】

図37は、S615により示されたトラップ型VP処理のサブルーチンプログラムを示すフローチャートである。S620により、新たなトラップ型VPの生成要求があったか否かの判断がなされ、ない場合にはS623へ進み、トラップ型VPが使用済みであるか否かの問合せがあったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。

【0222】

ブラウザフォン30がS598に従ってVP用IC端末19Vに新たなトラップ型VPの生成要求を出した場合には、S620によりYESの判断がなされて制御がS621へ進む。S621では、VP用IC端末19Vのトラップ型RFIDデータ領域の最後のVP氏名の暗号回数nを「1」加算して、VPの本名をn+1回秘密鍵で暗号化して新たなトラップ型VP氏名を生成する処理がなされる。たとえば図9の場合には、トラップ型RFIDデータ領域の最後のVP氏名E<sup>3</sup>(B13P)の暗号回数が3回であり、これに「1」加算して暗号回数4にし、VPの本名B13Pを4回暗号化して新たなトラップ型V



P氏名E<sup>4</sup> (B13P) を生成する処理がなされる。

【0223】

次にS622へ進み、その生成されたトラップ型VPを、ブラウザフォン30へ出力するとともに、トラップ型RFID領域における最後のVP氏名の次の空き領域に記憶させる処理がなされる。

【0224】

S590に従ってブラウザフォン30がVP用IC端末19Vに対し今アクセスしようとしているサイト(図30の自動決済しようとしている業社)にトラップ型VPが既に使用されているか否かの問合せを行なった場合には、S623によりYESの判断がなされて制御がS624へ進む。この問合せの際にはブラウザフォン30はVP用IC端末19Vに対し、今アクセスしようとしているサイト名(図30の自動決済しようとしている業社名)も併せて伝送する。S624では、トラップ型RFID領域(図9参照)を検索する処理がなされる。制御がS625へ進み、伝送されてきたサイト名(業社名)に対しトラップ型VP氏名が使用済みであるか否かの判断がなされる。たとえばブラウザフォン30から伝送されてきたサイト名(業社名)がMECであった場合には、図9を参照して、トラップ型VP氏名E<sup>2</sup> (B13P) が使用済みであることがわかる。

【0225】

トラップ型VP氏名が使用済みであると判断された場合には制御がS626へ進み、使用済みである旨をブラウザフォン30へ出力するとともに、S627により、使用されているトラップ型VPとそれに対応するトラップ型RFIDデータとをブラウザフォン30へ出力する処理がなされる。たとえば、図9の場合には、伝送されてきたサイト名(業社名)がMECであった場合には、トラップ型VPとしてE<sup>2</sup> (B13P) がブラウザフォン30へ出力されるとともに、トラップ型RFIDデータmecがブラウザフォン30へ出力される。

【0226】

図9のトラップ型RFID領域を検索した結果、ブラウザフォン30から伝送されてきたサイト名(業社名)に対しトラップ型VPが未だ使用されていない場合にはS625によりNOの判断がなされて制御がS628へ進み、未使用の旨をブラウザフォン30へ出力する処理がなされる。

【0227】

図38、図39は、コンビニエンスストア2のサーバ16の処理動作を説明するためのフローチャートである。S315により、VPの氏名、Eメールアドレス、金融機関の名称を受信したか否かの判断がなされ、受信していない場合にS316へ進み、VPが購入した商品を預かったか否かの判断がなされ、預かっていない場合にS317へ進み、商品の引取り操作があったか否かの判断がなされ、ない場合にはS318へ進み、その他の処理を行なった後S315へ戻る。

【0228】

このS315~S318のループの巡回途中で、決済サーバ10が誕生したVPの氏名、Eメールアドレス、当該金融機関の名称をコンビニエンスストア2へ送信した場合には(S18参照)、S315によりYESの判断がなされてS319へ進み、正当機関チェック処理がなされた後、S320へ進む。

【0229】

S320では、R=D<sub>KP</sub>(L)であるか否かの判断がなされ、正当機関でない場合にはNOの判断がなされてS321へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合にはS320によりYESの判断がなされてS322へ進み、受信データをデータベース17へ登録する処理がなされる。

【0230】

ユーザがVPとしてたとえば電子ショッピング等を行なってそのVPの住所であるコンビニエンスストア2に購入商品が配達されてコンビニエンスストア2がその商品を預かった場合には、S316によりYESの判断がなされてS316aへ進み、該当するVPの



商品預かり情報のアドレス領域に商品を預かった旨の情報を記憶させる処理がなされる。その際に、当該商品の決済が済んでいるか否かの情報も併せて記憶させる。次に制御が S 3 2 3 へ進み、当該 VP の E メールアドレスを割出し、その E メールアドレスへ商品を預かった旨のメールを送信する処理がなされる。VP は、その E メールを見ることにより、コンビニエンスストアに購入商品が配達されたことを知ることができ、その商品を引取るためにそのコンビニエンスストアに出向く。

#### 【0231】

ユーザが VP としてコンビニエンスストア 2 に出向き、配達された商品を引取るための操作を行えば、S 3 1 7 により YES の判断がなされる。そして制御が S 3 2 4 へ進み、VP 用 IC 端末 19 V の差込指示が表示される。それを見たユーザは、自己の VP 用 IC 端末 19 V を端末 7 3 の USB ポートへ差込んで接続する。すると、S 3 2 5 により YES の判断がなされて S 3 2 6 へ進み、暗証番号チェック処理がなされる。ユーザは、端末 7 3 に設けられているキーボードから VP 用の暗証番号を入力する。暗証番号が一致して適正であることを条件として、制御が S 3 2 7 へ進み、接続されている VP 用 IC 端末 19 V から VP 用の氏名を呼出してそれに基づいてデータベース 1 7 を検索する処理がなされる。そして、該当する VP の商品預かり情報のアドレス領域に、商品預かり情報が記録されているか否かの判断が S 3 2 8 によりなされる。商品預かり情報がなければ S 3 2 9 へ進み、預かり商品がない旨が表示される。一方、商品預かり情報がある場合には S 3 3 0 へ進み、電子証明書の出力要求が VP 用 IC 端末 19 V に対しなされる。VP 用 IC 端末 19 V は、それを受けて、記憶している電子証明書をサーバ 1 6 に出力する。すると、S 3 3 1 により YES の判断がなされて S 3 3 2 へ進み、出力されてきた電子証明書内の公開鍵 KP を読出し、S 3 3 3 により、本人チェック処理がなされる。

#### 【0232】

差込まれている VP 用 IC 端末 19 V は、前述したように、VP 本名に対する電子証明書は格納しているものの、トラップ型 VP に対する電子証明書は格納しておらず、そのトラップ型 VP に対する電子証明書は XML ストア 5 0 に格納されている。VP 本名を用いて電子ショッピング等を行なってその購入商品がコンビニエンスストア 2 へ届けられた場合には、S 3 2 7 に従って呼出された VP 氏名は VP の本名となる。その場合には、S 3 3 0 の要求に従って VP 用 IC 端末 19 V は電子証明書を出力することができる。その場合に S 3 3 1 により YES の判断がなされて制御が S 3 3 2 へ進む。一方、トラップ型 VP 氏名を用いて電子ショッピングを行ないその購入商品がコンビニエンスストア 2 へ届けられた場合には、その商品をトラップ型 VP としてコンビニエンスストア 2 へ引取りに行くこととなる。その場合には、S 3 2 7 によって VP 用 IC 端末 19 V から呼出される VP 氏名は、トラップ型 VP 氏名となる。その結果、そのトラップ型 VP 氏名に対応する電子証明書の出力要求が S 3 3 0 から VP 用 IC 端末 19 V に対し出される。その場合には、VP 用 IC 端末 19 V は、XML ストア 5 0 から電子証明書を取り寄せる旨の指示を出力する。

#### 【0233】

その出力があれば、制御が S 6 3 1 へ進み、XML ストア 5 0 へアクセスして該当する電子証明書を取り寄せる処理がなされた後制御が S 3 3 2 へ進む。

#### 【0234】

次に S 3 3 4 へ進み、 $R = D_{KP}(I)$  であるか否かの判断がなされる。正当でないなりすましの VP である場合には、S 3 3 4 により NO の判断がなされて S 3 3 5 へ進み、不適正である旨が表示される。一方、適正な VP であった場合には、制御が S 3 3 6 へ進み、預かり商品番号を表示し、S 3 3 7 により、その商品に関し決済済みであるか否かの判断がなされ、決済済みの場合には S 3 3 9 へ進むが、決済済みでない場合には S 3 3 8 へ進み、決済処理が行なわれる。

#### 【0235】

S 3 3 9 では、商品の引渡し完了したか否かの判断がなされる。コンビニエンスストア 2 の店員は、S 3 3 6 により表示された預かり商品番号を見て、該当する番号の商品を

探し出し、顧客にその商品を引渡しした後、商品引渡し完了操作を行なう。すると、S339によりYESの判断がなされてS340へ進み、データベース17の商品預かり情報のアドレス領域を更新し、商品預かりなしの状態にした後、S315へ戻る。

#### 【0236】

S326の暗証番号チェック処理は、図39(a)に示されている。S345により、暗証番号の入力指示が表示され、ユーザが入力すればS347へ進み、その入力された暗証番号をサーバ16に接続されているVP用IC端末19Vへ伝送し、その暗証番号の適否の判定結果がVP用IC端末19Vから返送されてくれば、S349へ進む。S349では、適正な判定結果か否かが判別され、不適正であればS350により不適正の表示を行なってS315へ戻るが、適正であればこのサブルーチンが終了して、制御がS327へ進む。

#### 【0237】

S333の本人チェック処理は、図39(b)に示されている。S355により、乱数Rを生成してVP用IC端末へ伝送する処理がなされ、チャレンジデータRに対するレスポンスデータIがVP用IC端末から返送されてくるまで待機する。Iが返送されてくれば、このサブルーチンが終了する。

#### 【0238】

S338の決済処理は、図39(c)に示されている。S359により、預かり商品の価格を表示する処理がなされ、S360へ進み、入金があるか否かの判断がなされる。ない場合にはS362へ進み、リロード金額による支払操作があったか否かの判断がなされ、ない場合にはS360へ戻る。そして、ユーザが現金による支払を行なってコンビニエンスストアの店員が入金があった旨の操作を行なえば、S360によりYESの判断がなされてS361へ進み、商品販売会社の口座へ入金処理を行なってこのサブルーチンプログラムが終了する。

#### 【0239】

一方、ユーザがVP用IC端末19に記憶されているリロード金額を使用して支払操作を行なうべくその旨の操作がなされれば、S362によりYESの判断がなされてS363へ進み、価格Gの引落し要求をVP用IC端末19Vへ伝送する処理がなされる。そしてS364へ進み、VP用IC端末19Vから引落し完了信号が出力されてきたか否かの判断がなされ、出力されてくるまで待機する。そして、引落し完了信号を受信すれば、S364によりYESの判断がなされてS361へ進む。

#### 【0240】

次に、別実施の形態を説明する。この別実施の形態は、ブラウザフォン30やユーザのパーソナルコンピュータ等のユーザ側端末およびIC端末19およびWebサイト(業社)によって、個人情報保護のシステムが完結する簡易型システムである。前述した実施の形態との相違は、トラップ型VPのEメールアドレスがVP本名のEメールアドレスと同じである。よって、トラップ型VP宛のEメールを金融機関7が転送する必要がない。またトラップ型VPの氏名は、そのトラップ型VPがアクセスするサイト(業社)の名称を、VP本名に用いられる秘密鍵で暗号化したものを用いる。トラップ型VPの口座番号やクレジット番号も、VPが本名として用いる口座番号、クレジット番号と同じものを用いる。

#### 【0241】

図40(a)は、VP用IC端末19VのEEPROM26のトラップ型RFID領域に格納されている情報を示す図である。このトラップ型RFID領域には、VP氏名として、VPの本名B13Pのみが記憶され、トラップ型VP氏名は何ら記憶されない。トラップ型VPの氏名は、トラップ型VPとしてアクセスしたサイト(業社)を本名のVPの秘密鍵KSBで暗号化したものを用いる。この暗号化回数は1回に限らず2回以上の或る定められた回数であってもよい。よって、トラップ型VPがアクセスしたサイト名(業社名)のみを記憶させることにより、そのサイト名(業社名)に対応するトラップ型VPの氏名は、わざわざ記憶させなくとも、EKSB(業社名)の演算式に従って必要に応じて

その都度算出することができる。トラップ型VPの秘密鍵は、トラップ型VPに対応するサイト名(業社名)を本名のVPの秘密鍵KSBで復号化したものを用いる。よって、トラップ型VPに対応させて逐一公開鍵や秘密鍵をVP用IC端末19Vに記憶させる必要はなく、秘密鍵=D<sub>KSB</sub>(業社名)の演算式に従って必要に応じてその都度算出することができる。よって、XMLストア50の「暗号回数」の記憶が不要となる。

#### 【0242】

図40(b)は、トラップ型VP処理のサブルーチンプログラムを示すフローチャートである。このサブルーチンプログラムは、図37に示したトラップ型VP処理の別実施の形態である。S960により、新たなトラップ型VPの生成要求がブラウザフォン30からあったか否かの判断がなされ、あった場合には制御がS959へ進み、アクセスするサイト(業社名)の名称の入力要求がブラウザフォン30へ出される。ブラウザフォン30からアクセスするサイト(業社)の名称が伝送されてくれば、制御がS957へ進み、その伝送されてきたサイト名(業社名)をVPの本名B13Pの秘密鍵KSBで暗号化して、新たなトラップ型VP氏名であるE<sub>KSB</sub>(業社名)を算出する処理がなされる。次に制御がS956へ進み、その算出した新たなトラップ型VP氏名をブラウザフォン30へ出力する処理がなされ、S954により、入力されたサイト名(業社名)をトラップ型RFID領域に記憶させる処理がなされる。

#### 【0243】

S953～S948は、図37に示したS623～S628と同じ制御のために、説明の繰返しを省略する。

#### 【0244】

図40(c)は、VP用IC端末19Vによって行なわれる個人情報流通チェックのサブルーチンプログラムを示すフローチャートである。S970により、Eメールの受信があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。トラップ型VP宛のEメールの受信があれば、ブラウザフォン30は、そのEメールデータをVP用IC端末へ入力する。すると制御がS969へ進み、その入力されたEメールの宛名をVPの本名に用いられる公開鍵KPBで復号化するD<sub>KPB</sub>(宛名)の演算を行ない、その演算結果がEメールの送信者名と一致するか否かの判断がなされる。

#### 【0245】

Eメールの宛名はトラップ型VP氏名となっており、そのトラップ型VP氏名は、そのトラップ型VPがアクセスしたサイト名(業社名)をVPの秘密鍵KSBで暗号化したものを用いている。よって、トラップ型VPがその氏名を用いてアクセスしたサイト(業社)からそのトラップ型VP宛にEメールが送信された場合には、S969によりYESの判断がなされる筈である。その場合には、S968により、適正である旨がブラウザフォン30へ出力され、ブラウザフォン30の表示部76によりその旨が表示される。一方、トラップ型VPがその氏名を用いてアクセスしたサイト(業社)以外のサイト(業社)からそのトラップ型VP氏名をEメールの宛名としてEメールが送信されてくれば、S969によりNOの判断がなされ、制御がS967へ進む。S967では、Eメールの宛名を本名のVPの公開鍵KPBで復号化する処理がなされる。その結果、Eメールの宛名であるトラップ型VP氏名が公開鍵KPBで復号化されて平文のサイト名(業社名)が算出されることとなる。このサイト名(業社名)は、Eメールの宛名に用いられているVP氏名としてアクセスしたサイト名(業社名)のことであり、アクセスしたサイト(業社)が個人情報をEメールの送信者に不正流通したことが考えられる。よって、S967により、D<sub>KPB</sub>(宛名)が不正流通し、送信者名の業者が不正入手した旨をブラウザフォン30へ出力する。ブラウザフォン30では、その旨を表示部76により表示させる。

#### 【0246】

図41は、購入済商品に付されているRFIDタグから発信されるRFIDを利用したサービスを行なうのに必要となる各業社からなる構成を示す構成図である。このRFIDを利用したサービス(以下「RFIDサービス」と言う)は、前述したサプライヤ群Sの1つである商品メーカー300と、会社群45の1つである中間流通業者301と、会社

群45の一つである商品情報サービス業社302と、加盟店群6の1つである小売店20bとにより提供可能となる。

#### 【0247】

商品メーカー300には、Webサーバ303とWebデータベース304とが設置されている。中間流通業者301には、Webサーバ305とWebデータベース306とが設置されている。商品情報サービス業社302には、Webサーバ307とWebデータベース308とが設置されている。小売店20bには、Webサーバ309とWebデータベース310とが設置されている。これら各Webサーバ303、305、307、309等が広域・大容量中継網43によりそれぞれ通信可能に構成されている。またRFIDサービスを受ける個人ユーザの自宅47が広域・大容量中継網43に接続されている。

。

#### 【0248】

図42は、商品情報サービス業社302のWebデータベース308に記憶されているデータの内容を示す図である。Webデータベース308には、RFIDタグメーカーが製造したRFIDタグから発信されるRFIDを記憶するエリアと、商品メーカー300や農産物を生産する農家等の生産者のURLを記憶するエリアと、中間流通業者301のURLを記憶するエリアと、小売店20bのURLを記憶するエリアと、個人ユーザ（購入者）専用のページを記憶するエリアとが設けられている。

#### 【0249】

図42の場合には、RFIDタグメーカーが製造したRFIDタグから発信されるRFIDとして、892013960～892014990が登録されている。そのうち、http//www.satoのURLの生産者の各生産品に付されるRFIDタグとして、892013960～892014560が割り振られている。http//www.isidaの生産者、http//www.katoの生産者も、図42に示すRFIDが割り振られている。

#### 【0250】

http//www.kaneiの中間流通業者には、http//www.satoの生産者とhttp//www.isidaの生産者からの生産品が入荷される。その入荷された段階で、両生産者の生産品に付されているRFIDタグから発信されるRFID892013960～892014801に対応して中間流通業者http//www.kaneiのURLが記録される。http//www.mituiの中間流通業者も同様に、http//www.katoの生産者からの生産品が入荷され、その生産品に対応するRFID892014802～892014990に対応するエリアに記憶される。

。

#### 【0251】

中間流通業者から小売店に商品が入荷されれば、その入荷された商品に付されているRFIDタグに対応するRFIDに対応してその小売店のURLが図示するように記憶される。尚、RFID892014802～892014990に関しては、小売店の記憶エリアに何らURLが記憶されていない。これは、これらのRFIDを発信するRFIDタグが付された商品がまだ小売店に入荷されていない流通段階であるためである。

#### 【0252】

購入者ページには、RFIDタグが付された商品を購入した購入者のVP名B13P、NPXA、IQX3等のVP情報と、それに対応してVPが書込んだ種々の情報とが記憶される。なお、本実施の形態においては、IPv6を用いる。

#### 【0253】

図43は、商品情報サービス業社302のWebサーバ307の制御動作を示すフローチャートである。SR1により、検索式を受信したか否かの判断がなされる。この検索式は、個人ユーザが商品を検索するためにブラウザフォン30等から入力してWebサーバ307へ送信して来る検索式のことである。検索式が送信されてきていない場合にはSR2へ進み、新RFIDの登録要求があったか否かの判断がなされる。RFIDタグのメー

カーが新たなRFIDタグを製造してそのRFIDを商品情報サービス業社302のWebデータベースに登録すべく登録要求をWebサーバ307へ送信すれば、SR2によりYESの判断がなされてSR10へ進み、その送信されて来た新RFIDをWebデータベース308へ登録する処理がなされる。

#### 【0254】

商品メーカー300や農産物を生産する生産者から、自己の生産品に付するRFIDタグのRFIDを割り振ってもらうための申し込みがあったか否かの判断がSR3によりなされ、あった場合にはSR11へ進み、割り振りの申し込み個数だけRFIDを生産者に割り振って発行する処理がなされる。次にSR12へ進み、その割り振ったRFIDに対応させて生産者のURLをWebデータベースに記憶して登録処理がなされる。これにより、図42に示した商品ホームページには、記憶された生産者のURLが掲載されて表示されることとなる。

#### 【0255】

中間流通業者301からRFIDの申し込みがあったか否かがSR4により判断される。生産者が生産した生産品が中間流通業者301に入荷された場合にその入荷された商品に付されているRFIDタグのRFIDを中間流通業者301が読み取って、そのRFIDを商品情報サービス業社302のWebサーバ307へ送信する。すると、SR4によりYESの判断がなされてSR13へ進み、その送信されてきたRFIDに対応させて中間流通業者は301のURLをWebデータベース308に記憶して登録する処理がなされる。その結果、図42に示された商品ホームページに、その中間流通業者のURLが掲載されて表示されることとなる。

#### 【0256】

小売店20bからRFIDの申し込みがあったか否かがSR5により判断される。中間流通業者301から商品が小売店20bに入荷され、小売店20bによりその入荷商品に付されているRFIDタグのRFIDが読取られてそのRFIDがWebサーバ307へ送信されれば、SR5によりYESの判断がなされてSR14へ進み、その送信されてきたRFIDに対応させて小売店のURLをWebデータベース308へ登録する処理がなされる。その結果、図42の商品ホームページにその小売店のURLが掲載されて表示されることとなる。

#### 【0257】

SR5によりNOの判断がなされた場合には図44のSR6へ進む。SR6により、購入者からの書込み要求があったか否かの判断がなされる。あった場合には、SR15へ進み、正当期間証明処理がなされる。この正当期間証明処理の詳細は、図24(b)に示されている。次に、SR16へ進み、本人確認処理を行なう。この本人確認処理の詳細は、例えば、図18のS412～S417と同様の処理である。次にSR17へ進み、本人確認処理の結果正しいことの確認ができたか否かの判断がなされ、確認できない場合にはSR18により拒絶処理を行なった後SR1へ戻る。正しい確認ができた場合にはSR19へ進み、RFIDの送信要求を個人ユーザのブラウザフォン30へ伝送する処理がなされる。個人ユーザは、自己が購入した商品に付されているRFIDタグからRFIDを読み取り、それをブラウザフォン30からWebサーバ307へ送信する。すると、SR20によりYESの判断がなされてSR21へ進み、その送信されてきたRFIDに対応する購入者ページを作成して商品ホームページに掲載するとともに、その作成された購入者ページに対応する箇所に当該個人ユーザによるメッセージ等の書込みを許容する処理がなされる。個人ユーザは、自己のVP名、VPの住所（コンビニエンスストアの住所）、VPのEメールアドレス等のVP情報を書込むことができる。その他として、そのRFIDに対応する購入商品の使用後の感想等、当該商品を中古品として販売したい旨のメッセージ、当該商品を他の個人ユーザの商品と物々交換したい旨のメッセージ等が考えられる。使用後の感想が書きこまれることによって、他の一般消費者が商品購入の際に、その感想を参考にして判断することができると共に、その商品のメーカーが次の商品を開発する際にその感想等を参考にして商品開発をすることが可能となる。更に他の例としては、商品の購

入者が、購入者ページを商品に関するメモ代わりに利用することが考えられる。例えば、炊飯器で炊き込み御飯を炊いた時に少し水の分量が多かった場合に、その炊飯器に対応するRFIDの購入者ページの欄に、「米と水の比を4:5にして炊き込み御飯を炊いたが、少し水の分量が多かった」旨を書込んでおき、次の炊き込み御飯を炊く時の参考にできるようにする。

**【0258】**

更なる他の例としては、商品の取り扱い説明書、契約書、保証書等の情報をその対応するRFIDを購入者ページに記憶させておいてもよい。

**【0259】**

SR6によりNOの判断がなされた場合にはSR23へ進み、生産者からの追加情報書込みの要求があったか否かの判断がなされる。生産者は、販売された商品に関して、そのバージョンアップ情報、付属商品の出荷情報、メーカー側が欠陥を発見した場合の欠陥通知情報等を追加情報として生産者自身のホームページに掲載する。そして、自己のホームページに商品の追加情報を掲載したことを図42の商品ホームページに掲載してもらうべく、生産者は、Webサーバ307へ追加情報の書込み要求を送信する。するとSR23によりYESの判断がなされてSR24へ進み、追加情報が掲載された旨を商品ホームページに掲載する処理がなされる。また、商品が例えばパーソナルコンピュータのソフトであった場合に、そのソフトのバージョンアップ情報やバージョンアップされたソフトを有償または無償でダウンロードできるようにホームページに掲載してもよい。

**【0260】**

消費者から商品ホームページを閲覧したい旨の要求がWebサーバ307に送信された場合には、SR7によりYESの判断がなされてSR22へ進み、図42に示された商品ホームページを表示する処理がなされる。その商品ホームページを閲覧した消費者は、例えば図42に示すRFID892013960の商品について生産者から商品情報を入手したい場合には、<http://www.sato>の生産者URLをクリックする。すると生産者のホームページに自動的にアクセスでき、RFID892013960に対応する商品に関する種々の商品情報を閲覧することが可能となる。例えば、その商品が農産物等の食材の場合には、その食材の各種料理方法、栄養、カロリー、体への効用、生産農家、使用農薬、生産農家からのメッセージ等を閲覧できる。また、生産農家において、田植え代金や果樹園でのぶどう狩りや梨狩り体験等のイベント企画をホームページに掲載して消費者が閲覧できるようにする。

**【0261】**

個人ユーザが商品の検索を行なうべくブラウザフォン30から商品検索用の検索式を入力してWebサーバ307へ送信すれば、SR1によりYESの判断がなされてSR8へ進み、送られてきた検索式に従ってWebデータベース308を検索する処理がなされ、その検索結果をSR9により個人ユーザのブラウザフォン30へ返信する処理がなされる。ブラウザフォン30から送信されてくる検索式は、例えば、商品種類の指定、商品生産者の指定、性能(機能)の指定等を特定するものであり、その検索式に従ってSR8により、条件を満たす商品を割出してその商品情報とその商品に対応するRFID等をSR9により返信する。商品の検索に際しては、購入者ページ(図42参照)に書込まれている商品購入者の使用後の感想等も商品検索の一情報として利用される。更に、送られてくる検索式中には、その商品が販売されているまたは販売される予定の小売店を指定するデータも含まれている。そして、その検索式の条件を満たす商品のRFID全てを個人ユーザのブラウザフォン30へ返信する。

**【0262】**

図45は、個人ユーザのブラウザフォン30により商品を検索して購入するためのプログラムを示すフローチャートである。SQ1により、個人ユーザがブラウザフォン30から商品検索操作を行なったか否かの判断がなされる。行なった場合にはSQ2へ進み、商品を検索するための検索式の入力受付処理が行われる。個人ユーザは、ブラウザフォン30のキーを操作して商品検索式を入力する。次にSQ3へ進み、その入力した検索式を



Webサーバへ送信する処理が行なわれる。次に、SQ4へ進み、検索結果がWebサーバ307から返信されてきたか否かを判断し、返信されてくるまで待機する。

**【0263】**

Webサーバ307により検索結果が返信されて来ればSQ5へ進み、その検索結果をブラウザフォン30により表示する処理がなされる。次にSQ6へ進み、個人ユーザが再検索操作を行なったか否かの判断がなされる。個人ユーザは、返信されてきた検索結果を見て、それに満足しない場合には再度検索式を変更する等して再検索操作を行なう。すると、SQ2からSQ5の処理が繰り返し行なわれることとなる。

**【0264】**

次にSQ7へ進み、返信されてきた検索結果に含まれているRFIDの内のいずれかをブラウザフォン30に記憶させるための操作が行なわれたか否かの判断がなされる。個人ユーザが返信されてきた商品中に気に入った物がありかつその商品が自己の希望する小売店（最寄りの小売店等）により販売されている場合または販売される予定の場合には、その商品に対応するRFIDをブラウザフォン30に記憶させる操作を行なう。すると、SQ8へ進み、その指定されたRFIDをブラウザフォンがEEPROM194に記憶する処理を行なう。そして、個人ユーザは、その商品が売られている小売店に出向いて、ブラウザフォン30に記憶されているRFIDと一致するRFIDが発信されるRFIDタグが付されている商品を探し出して購入する。このようなRFIDに基づいて小売店で商品を探し出す方法としては、小売店20bのWebサーバ309へその記憶しているRFIDを送信し、Webサーバ309によりそのRFIDに対応する商品が陳列されている場所を割出して個人ユーザにその場所を知らせる。そして個人ユーザがその場所に出向き、そこに陳列されている商品のRFIDを読み取って記憶しているRFIDと照合して一致するか否かを逐一判別する方法を採用する。

**【0265】**

一方、返信されてきた検索結果中に含まれている商品の何れかを個人ユーザが気に入ってその商品をその製品の生産者から直接購入したい場合には、直接購入操作をブラウザフォン30により行なう。すると、SQ9によりYESの判断がなされてSQ10へ進み、その商品の生産者のホームページにアクセスする処理がなされる。次にSQ11に進み、正当期間チェック処理が行なわれる。この正当期間チェック処理の詳細は、図50(a)に基づいて後述する。次にSQ12へ進み、正当期間チェック処理の結果その商品の生産者から送信されてきた乱数Rを受信した電子証明書内の公開鍵KPを用いて算出された $D_{KP}(L)$ とが一致するか否かの判断がなされる。一致しない場合にはSQ14により、正当期間でない旨の警告表示がブラウザフォン30によりなされる。一方、一致する場合にはSQ13により、本人証明処理が行なわれた後SQ15へ進む。この本人証明処理は、例えば図35(c)にその詳細が示されている。

**【0266】**

SQ15では、個人ユーザのVP情報を生産者（商品メーカー）300のWebサーバ303へ送信する処理がなされる。このVP情報は、ブラウザフォン30に装着されているVP用IC端末19bのEEPROM26に記憶されているVP氏名・住所、VPのEメールアドレス等である。次にSQ16へ進み、購入したい商品に対応するRFIDを指定して直接購入を申し込む旨の情報をWebサーバ303へ送信する。次にSQ17へ進み、VP用決済処理がなされる。このVP用決済処理の詳細は、図53に示されている。この決済処理が終わった後、商品の生産者はRFIDにより指定された商品をVP（コンビニエンスストアの住所）へ配送する。個人ユーザは、そのコンビニエンスストアに出向いてVPとしてその商品を引取る。

**【0267】**

返信されてきた検索結果中に気に入った商品がありその商品を予約購入したい場合には、個人ユーザはブラウザフォン30によりRFIDを指定して購入予約操作を行う。この購入予約は、商品の生産者（商品メーカー）300に対して商品の購入を事前に予約しておくためのものである。購入予約操作があった場合にはSQ20へ進み、小売店の指定操



作があったか否か判断され、あるまで待機する。個人ユーザがブラウザフォン30により、商品を購入したい小売店（最寄りの小売店等）を指定する操作を行えば、SQ21へ進み、希望する商品の生産者のホームページにアクセスする処理がなされる。次にSQ22～SQ25の前述と同様の正当期間をチェックする処理がなされる。SQ24による本人証明処理が行われた後SQ26に進み、購入予約したいRFIDを指定された小売店等を生産者（商品メーカー）300のWebサーバ303へ送信する処理が行われる。次にSQ27へ進み、指定された小売店での価格を受信したか否かの判断がなされ、受信するまで待機する。後述するように、商品メーカー300のWebサーバ303は、購入予約したいRFIDと購入希望の小売店とを受信すれば、その小売店での販売価格を割出してブラウザフォン30へ返信する。すると、SQ28へ進み、受信した価格をブラウザフォン30により表示する処理がなされ、SQ29により購入OKの操作がなされたか否かの判断がなされ、なされていない場合にはSQ33により購入キャンセルの操作がなされたか否かの判断がなされ、なされていない場合にはSQ29に戻る。このSQ29、SQ30のループの巡回途中で、個人ユーザがブラウザフォン30により購入OKの操作を行えば、SQ31へ進み、購入予約時に指定したRFIDをブラウザフォン30のEEPROM194に記憶する処理がなされる。個人ユーザは、希望する商品が指定した小売店に入荷されたか否かを図42の商品ホームページを閲覧することにより知ることができる。また、RFIDにより指定された商品が指定された小売店に入荷された時点で商品情報サービス業社302のWebサーバ307からその個人ユーザのブラウザフォン30へ小売店に入荷した旨の情報を送信して個人ユーザに知らせるようにしてもよい。一方、個人ユーザがブラウザフォン30により購入キャンセル操作を行えば、SQ31を行うことなくこのサブルーチンプログラムは終了する。

#### 【0268】

個人ユーザが中古品の入手を希望する場合にその旨の操作をブラウザフォン30により行えば、SQ19によりYESの判断がなされてSQ32へ進み、該当する購入者ページ（図42参照）にアクセスする処理がなされる。次にSQ33へ進み、物々交換希望であるか否かの操作をブラウザフォン30により行う。物々交換の場合にはSQ35へ進み、自己が所有している交換したい商品のRFIDをブラウザフォン30により読取ってそれを送信する処理がなされる。そのRFIDを受信した個人ユーザは、そのRFIDをWebサーバ307へ送信して商品ホームページを検索し、該当する生産者のホームページにアクセスする等して商品情報を入手する。そして交換するか否かを返信する。交換する場合即ち取引が成立する場合にはSQ36によりYESの判断がなされてSQ37により物々交換処理を行う。

#### 【0269】

一方、物々交換ではなく有償による中古品の購入をブラウザフォン30により入力した場合には、SQ33によりNOの判断がなされてSQ34へ進み、有償による購入処理が行われる。

#### 【0270】

図47は、生産者（商品メーカー）300のWebサーバ303の制御動作を示すフローチャートである。SS1により、アクセスがあったか否かの判断がなされる。アクセスがあった場合にはホームページを表示する。次にSS3へ進み、予約購入要求があったか否かの判断がなされる。ない場合にはSS4へ進み、直接購入要求があったか否かの判断がなされる。ない場合にはSS20へ進みその他の処理がなされる。

#### 【0271】

前述したSQ18による予約購入の要求がブラウザフォン30から送信されてくれば、制御がSS5へ進み、前述と同様の正当期間証明処理がなされ、次にSS6へ進み、前述と同様の本人確認処理がなされ、SS7により本人確認の結果正しいか否かの判断がなされる。正しくない場合にはSS8による拒絶処理がなされる。一方、正しい場合にはSS9へ進み、RFIDと小売店との受信があったか否かの判断がなされ、あるまで待機する。ブラウザフォン30から前述のSQ26による購入予約したいRFIDと購入希望の小

売り店とが送信されてくれば、SS10へ進み、その小売店への直接出荷個数に達しているか否かの判断がなされる。その小売店に出荷する商品個数がある程度の量に達している場合には、中間流通業者を省いて商品メーカー300から直接小売店に商品を出荷できる。その直接出荷個数に達しているか否かの判断がこのSS10によりなされる。達している場合にはSS11へ進み、中間流通業社を省いた直接小売店への出荷に基づく価格をブラウザフォン30に返信する。一方、SS10により直接出荷個数に達していないと判断された場合にはSS12へ進み、中間流通業者を省くのに必要な予約個数、現在の予約個数、中間流通業者を省いた価格及び省かなかった価格をブラウザフォン30に返信する。

#### 【0272】

前述のSQ9に従った直接購入の要求がブラウザフォン30から送信されてくれば、前述と同様のSS13による正当機関証明書処理がなされ、SS14による本人確認処理がなされ、SS15による正しいか否かの判断がなされ、正しくなければSS16による拒絶処理がなされ、正しい場合にはSS17へ進む。

#### 【0273】

SS17では、VP情報とRFIDを受信したか否かの判断がなされ、受信するまで待機する。前述したSQ15によるVP情報が送信されSQ16によるRFIDがブラウザフォン30から送信されてくれば、制御がSS18へ進み、その送信されてきたRFIDに対応する商品の決済処理を行う。次にSS19により、商品をVPの住所（コンビニエンスストアの住所）へ配達するための処理がなされる。

#### 【0274】

図48は、S585により示された住所、氏名、Eメールアドレスの送信処理のサブルーチンプログラムを示すフローチャートである。この処理は、前述の自動決済処理（図31参照）の際に業者側からVP情報の送信要求があった場合等に実行される。S700により、業社側から住所、氏名、Eメールアドレスの送信要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。あった場合には制御がS701へ進み、その業社に使用しているVPの氏名、住所、Eメールアドレスを送信する処理がなされる。たとえば図9に示す例の場合には、業社MTTに使用しているVP氏名はE（B13P）であるために、この氏名E（B13P）を送信する。住所は、B13Pの住所すなわち□△○である（図3参照）。Eメールアドレスは、金融機関7がトラップ型VP用として開設しているEメールアドレス△△△△△△が送信される。

#### 【0275】

図49はS101に示されたVP出生依頼処理のサブルーチンプログラムを示すフローチャートである。このVP出生依頼は、PVを新たに誕生させるための依頼をVP管理サーバ9へ出すための処理である。S140により、暗証番号のチェック済みであるか否かの判断がなされ、適正な暗証番号である旨のチェックが済んでいる場合にはS141へ進むが、適正な暗証番号のチェックが未だ済んでいない場合にはこのサブルーチンプログラムが終了する。適正な暗証番号である旨のチェックが済んでいる場合にはS141へ進みV出生要求の操作があったか否かの判断がなされる。ユーザがブラウザフォン30のキーボードを操作してVP出生要求の操作を行えば、制御がS142へ進み、VP出生依頼要求を金融機関7のVP管理サーバ9へ送信する処理がなされる。次にS143へ進み、正当機関チェック処理がなされる。この正当機関チェック処理は、相手側の機関（この場合には金融機関7）が正当な機関であるか否かをチェックするものであり、金融機関7になりすまして対応する不正行為を防止するためのものであり、図50（a）にそのサブルーチンプログラムが示されている。

#### 【0276】

先に、図50（a）に基づいて正当機関チェック処理のサブルーチンプログラムを説明する。この正当機関チェック処理は、図24（b）に示された正当機関証明処理に対応するチェック側のプログラムである。まずS160により、電子証明書を受信したか否かの判断を行ない、受信するまで待機する。正当機関証明処理では、図24（b）に示されているように、S90により電子証明書が送信される。この電子証明書が送信されてくれば

、制御がS161へ進み、乱数Rを生成して送信する処理がなされる。すると、機関側では、図24(b)に示すようにS92により、当該機関の秘密鍵SKを用いて受信した乱数Rを暗号化してLを算出して送信する処理が行なわれる。このRの暗号化データLをブラウザフォン30が受信すれば、制御がS163へ進み、受信した電子証明書内の公開鍵KPを用いてLを復号化する処理すなわち $D_{KP}(L)$ を算出する処理が行なわれる。

#### 【0277】

そして、図49のS144へ進み、 $R=D_{KP}(L)$ であるか否かの判断がなされる。正当な機関である場合には、 $R=D_{KP}(L)$ となるはずであり、その場合にはS146へ進むが、他人が金融機関7になしすましている場合には、S144によりNOの判断がなされ、S145へ進み、正当機関でない旨の警告表示がブラウザフォン30によりなされてこのサブルーチンプログラムが終了する。

#### 【0278】

正当機関であることが確認された場合には、S146へ進み、RPの氏名、住所の入力要求を受信したか否かの判断がなされ、受信するまで待機する。VP管理サーバ9では、前述したように、VP出生依頼要求を受信すれば、RPの氏名、住所の入力要求を送信するのであり(S2参照)、そのRPの氏名、住所の入力要求をブラウザフォン30が受信すれば、S146によりYESの判断がなされて制御がS147へ進む。

#### 【0279】

S147では、RPの氏名、住所の入力指示をブラウザフォン30のディスプレイに表示する処理がなされ、入力があるまで待機する(S148)。入力があった段階でS149へ進み、その入力データを金融機関7のVP管理サーバ9へ送信する処理がなされる。

#### 【0280】

次にS150へ進み、本人証明処理が行なわれる。この本人証明処理は、VP出生依頼を行なったユーザが本人自身であるか否かを証明するための処理であり、図54(a)にそのサブルーチンプログラムが示されている。ここで、図54(a)に基づいて、その本人証明書のサブルーチンプログラムを説明する。

#### 【0281】

この本人証明処理は、前述したS4、S62等に基づいて乱数Rが送信されてきた場合にその乱数に基づいて本人証明を行なうためのものである。まずS125により、乱数Rを受信したか否かの判断がなされ、受信するまで待機する。乱数Rを受信した場合にはS216へ進み、その受信した乱数RをIC端末19Rまたは19Vへ送信する処理がなされる。IC端末では、後述するように、記憶している認証鍵KNまたは公開鍵KPを用いて乱数Rを暗号化してレスポンスデータIを生成して出力する処理が行われる。そのレスポンスデータIが出力されてくれば、S217によりYESの判断がなされてS218へ進み、そのIをVP管理サーバ9へ送信する処理がなされる。

#### 【0282】

図29に示すVP出生依頼処理を行なう場合には、ブラウザフォン30のUSBポート18にVP用IC端末19Vを接続している。そして、VP出生依頼処理の際の本人証明処理では、VP用IC端末19Vに記憶されているRPの認証鍵KNを用いて乱数Rを暗号化する処理がなされる。これについては、後述する。

#### 【0283】

その結果、図49のS150のVP出生依頼処理の際の本人証明では、RPであることの証明がなされる。

#### 【0284】

次にS151へ進み、アクセス拒絶を受信したか否かの判断がなされ、アクセス拒絶を受信した場合にS152へ進み、アクセス拒絶の表示が行なわれる。一方、アクセスが許容された場合にはS153へ進み、VP出生依頼を行なったユーザが希望するコンビニエンスストア2の入力があるか否かの判断がなされる。出生したVPの住所が、コンビニエンスストア2の住所となるために、ユーザは、自己の希望するコンビニエンスストア2がある場合には、そのコンビニエンスストア2を特定する情報をブラウザフォン30のキー

ボードから入力する。入力があれば、S154により、その希望のコンビニエンスストア2のデータがVP管理サーバ9へ送信される。希望のコンビニエンスストア2の入力がなかった場合には、前述したように、RPの住所に最も近いコンビニエンスストア2の住所が出生したVPの住所となる。

#### 【0285】

次にS155へ進み、VPの公開鍵の送信要求があったか否かの判断がなされ、あるまで待機する。VP管理サーバ9では、前述したように、VPの出生依頼があった場合に、VPの公開鍵の送信要求を出す(S30参照)。その送信要求をブラウザフォン30が受ければ、制御がS156へ進み、VP用IC端末19Vへ公開鍵出力要求を出す。すると、VP用IC端末19Vが、記憶しているVPの公開鍵KPを出力する。その出力があれば、制御がS158へ進み、その出力された公開鍵KPを金融機関7のVP管理サーバ9へ送信する。

#### 【0286】

図50(b)は、S105に示された電子証明書発行要求処理のサブルーチンプログラムを示すフローチャートである。S165により、適正な暗証番号である旨のチェックが済んでいるか否かの判断がなされ、未だに済んでいない場合にはこのサブルーチンプログラムが終了する。一方、適正な暗証番号である旨のチェックが済んでいる場合にはS166へ進み、RP用電子証明書の発行依頼操作があったか否かの判断がなされる。ユーザがブラウザフォン30のキーボードを操作して発行依頼を行なった場合には、制御がS167へ進み、RPの住所、氏名の入力指示が表示される。ユーザがキーボードより入力すれば、制御がS169へ進み、RP用IC端末19Rから公開鍵KPを呼出す処理がなされる。この電子証明書発行要求処理を行なう場合には、ユーザは、ブラウザフォン30のUSBポート18に自己のRP用IC端末19Rを接続しておく必要がある。そして、S169の処理が行なわれた場合には、その接続されているRP用IC端末19Rが記憶しているRP用の公開鍵KPがブラウザフォン30に出力され、S170により、その出力されてきた公開鍵KPと入力されたRPの住所、氏名とが金融機関7の認証用サーバ11へ送信される。

#### 【0287】

図51(a)はS102に示されたVP用入力処理のサブルーチンプログラムを示し、図51(b)はS106に示されたRP用入力処理のサブルーチンプログラムを示すフローチャートである。

#### 【0288】

VP用入力処理が行なわれる場合には、ブラウザフォン30のUSBポート18にVP用IC端末19Vを接続しておく必要がある。S175により、適正な暗証番号である旨のチェックが終了しているか否かの判断がなされ、適正な暗証番号のチェックが未だなされていない場合にはこのサブルーチンプログラムが終了する。適正な暗証番号のチェック済の場合には、S176へ進み、VP用入力操作があったか否かの判断がなされる。前述したように、金融機関7のVP管理サーバ9によりVPの出生処理が行なわれた場合には、誕生したVPの氏名、住所(コンビニエンスストア2の住所)、コンビニエンスストア2の名称、Eメールアドレス、電子証明書が記憶されたIC端末19Iが郵送されてくるのであり、そのIC端末19Iをユーザがブラウザフォン30に挿入すれば、S176によりYESの判断がなされてS178へ進み、そのIC端末19Iの記録データが読込まれて接続されているVP用IC端末19Vへ伝送される。

#### 【0289】

ユーザがブラウザフォン30のキーボードからVP用ユーザエージェントの知識データの入力操作を行なえば、S177によりYESの判断がなされてS179へ進み、入力された知識データをVP用IC端末19Vへ伝送する処理がなされる。

#### 【0290】

ユーザが金融機関7の自己の口座から資金を一部引落しすれば、その引落とし額Gがブラウザフォン30へ送信されてくる(S69参照)。その引落とし額Gがブラウザフォン30

に入力されれば、S180によりYESの判断がなされてS181へ進み、引落し額GをVP用IC端末19Vへ転送してリロード金額として加算記憶させる処理がなされる。

#### 【0291】

RP用入力処理が行なわれる場合には、ブラウザフォン30のUSBポート18にRP用IC端末19Rを接続しておく必要がある。まずS185により、適正な暗証番号のチェックが済んでいるか否かの判断がなされ、済んでいる場合にはS186へ進み、RPの電子証明書を受信したか否かの判断がなされる。ユーザがRPの電子証明書の発行依頼を認証用サーバに対し行なえば、前述したように、RPの電子証明書が作なされてブラウザフォン30に送信されてくる（S28参照）。その電子証明書が送信されてくれば、S186によりYESの判断がなされてS187へ進み、受信した電子証明書をRP用IC端末19Rへ伝送して、RP用IC端末へ記憶させる処理がなされる。

#### 【0292】

ユーザがブラウザフォン30のキーボードを操作して、RP用ユーザエージェントの知識データの入力操作を行なえば、S188によりYESの判断がなされてS189へ進み、その入力された知識データをRP用IC端末19Rへ伝送する処理がなされ、RP用IC端末19Rがその入力された知識データを記憶する。

#### 【0293】

ユーザが決済サーバ10に対し自己の口座内の資金の一部を引落す引落し要求を行なった場合には、前述したように、引落し金額であるGが決済サーバ10からユーザのブラウザフォン30へ送信される。すると、S190によりYESの判断がなされてS191へ進み、引落し額GをRP用IC端末19Rへ伝送し、リロード金額としてGを加算更新する処理が行なわれる。

#### 【0294】

図52は、ユーザ（RPとVPが存在する）がクレジットカードの支払を行なってSETに従った決済が行なわれる場合の全体概略システムを示す図である。まず、カード会員がクレジットカードの発行手続を行なえば、クレジットカード発行会社4に設置されているサーバが、クレジットカード発行の申込みがあったことを判別して、当該カード会員に対しクレジットカード番号を発行する。その際に、カード会員がVP用のクレジットカードの発行を要求した場合には、クレジットカード発行会社4のサーバは、そのVPの氏名や住所等のデータを入力してもらい、そのデータに基づいて金融機関などに登録されているVPか否かを金融機関7に問合せ。そして、金融機関7のデータベース12に記憶されている正規のVPであることが確認されたことを条件として、クレジットカード発行会社4のサーバは、そのVPに対しクレジット番号を発行する処理を行なう。

#### 【0295】

つまり、クレジットカード発行会社4のサーバは、仮想人物用のクレジット番号を発行するクレジット番号発行ステップを含んでいる。また、仮想人物用のクレジット番号を発行するクレジット番号発行手段を含んでいる。さらに、このクレジット番号発行ステップまたはクレジット番号発行手段は、前述したように、クレジット番号発行対象となる仮想人物が前記所定機関に登録されている正規の仮想人物であることが確認されたことを条件として、前記クレジット番号を発行する。クレジットカード発行会社4によって発行されたクレジットカード（RP用とVP用の2種類存在する）を所持するユーザは、SETによる取引をするための会員の登録要求を認証用サーバ11に出す。認証用サーバ11は、そのユーザがクレジットカード発行会社4のクレジット会員であるか否かの認証要求をクレジットカード発行会社4に出す。クレジットカード発行会社4からクレジットカードの会員である旨の認証の回答が認証用サーバ11に返信されてくれば、認証用サーバ11は、SET用の電子証明書を作成してカード会員に送る。

#### 【0296】

電子モール等の加盟店6がSETによる取引を可能にするためには、まず、SETによる取引のための会員登録要求を認証用サーバ11に出す。認証用サーバ11では、加盟店6が契約している加盟店契約会社（アクアイアラ）5に、当該加盟店6が正当な契約会社

であるか否かの認証要求を送信する。加盟店契約会社 5 から正当な加盟店である旨の回答が返信されてくれば、認証用サーバ 11 は、その加盟店 6 のための S E T 用の電子証明書を作成して加盟店 6 に発行する。

#### 【0297】

この状態で、カード会員が加盟店 6 により電子ショッピングを行なって S E T により取引を行なう場合には、まず商品やサービス等の購入要求をカード会員が加盟店 6 へ送信する。加盟店 6 では、その購入要求を承認してよいか否かの承認要求を支払承認部 33 からペイメントゲートウェイ 27 を介してクレジットカード発行会社 4 へ送信する。クレジットカード発行会社 4 から承認の回答がペイメントゲートウェイ 27 を介して加盟店 6 に返信されてくれば、加盟店 6 は、購入を受理した旨をカード会員に送信する。また加盟店 6 は、支払要求部 34 から支払要求をペイメントゲートウェイ 27 に送信する。ペイメントゲートウェイ 27 は、その支払要求に応じた決済要求をクレジットカード発行会社 4 へ送信するとともに、支払回答を加盟店 6 へ返信する。

#### 【0298】

カード会員と加盟店 6 との間では、商品やサービスの購入取引を行なう際に、互いの電子証明書を送信して、正当な本人である旨の確認が行なわれる。

#### 【0299】

クレジットカード発行会社 4 が、ユーザとしての R P にクレジットカードを発行した場合には、そのクレジットカード番号等のカード情報が当該ユーザの R P 用 I C 端末 19 R に入力されて記憶される。一方、ユーザが V P としてクレジットカード発行会社 4 からクレジットカードの発行を受ける際には、V P 用に発行された電子証明書をクレジットカード発行会社 4 に送信し、金融機関 7 による身分の証明を行なってもらい必要がある。その上で、クレジットカード発行会社 4 がクレジットカードを発行した場合には、そのクレジットカードのカード番号等のカード情報が当該ユーザの V P 用 I C 端末 19 V に入力されて記憶される。

#### 【0300】

前述した S E T 用の電子証明書の発行も、R P 用と V P 用との 2 種類のケースに分けて発行される。そしてそれぞれ発行された S E T 用の電子証明書が、それぞれの I C 端末 19 R または 19 V に入力されて記憶される。

#### 【0301】

図 53 は、S 103 に示した V P 用決済処理のサブルーチンプログラムを示すフローチャートである。まず S 195 により、適正な暗証番号である旨のチェックが終了しているか否かの判断がなされ、終了していなければこのサブルーチンプログラムが終了し、適正な暗証番号のチェック済の場合には S 196 へ進む。

#### 【0302】

この V P 用決済処理は、金融機関 7 のユーザの銀行口座内の資金の一部を引落して V P 用 I C 端末 19 V へリロードする処理と、デビットカードを使用して決済を行なう処理と、クレジットカードを使用して決済を行なう処理と、V P 用 I C 端末 19 V へリロードされているリロード金額を使用して決済を行なう場合とを有している。

#### 【0303】

ユーザが自己の銀行口座内の資金を一部引落して V P 用 I C 端末へリロードする操作を行なえば、S 197 により、その引落し要求が金融機関 7 の決済サーバ 10 へ送信される。次に S 198 へ進み、正当機関チェック処理 (図 30A 参照) が行なわれる。

#### 【0304】

次に S 199 へ進み、 $R = D_{KP}(L)$  である否かの判断がなされ、正当機関でない場合には S 119 により NO の判断がなされて S 200 へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合には、 $R = D_{KP}(L)$  となるために、制御が S 201 へ進み、氏名の入力要求があったか否かの判断がなされ、あるまで待機する。前述したように、決済サーバ 10 は、I C 端末への引落し要求があった場合には、氏名の入力要求を送信する (S 60 参照)。この氏名の入力要求が送信されてくれば、S 201 により



YESの判断がなされてS202へ進み、VP用IC端末19VからVPの氏名を呼出して決済サーバ10へ送信する処理がなされる。次にS203へ進み、本人証明処理（図34A参照）がなされる。

#### 【0305】

次にS204へ進み、引落し額の入力要求があったか否かの判断がなされ、なければS205へ進み、不適正な旨の返信があったか否かの判断がなされ、なければS204へ戻る。この204、205のループの巡回途中で、決済サーバ10がユーザの正当性が確認できないと判断した場合には不適正である旨の返信を行なう（S79参照）。その結果、S205によりYESの判断がなされてS207へ進み、不適正である旨がブラウザフォン30のディスプレイにより表示される。一方、決済サーバ10が本人認証の結果正当な本人であると判断した場合には引落し額の入力要求をブラウザフォン30へ送信する（S87参照）。すると、S204によりYESの判断がなされてS206へ進む。

#### 【0306】

S206では、引落し額の入力指示をブラウザフォン30のディスプレイに表示させる処理がなされる。ユーザがキーボードから引落し額を入力すれば、S208によりYESの判断がなされてS209へ進み、その入力された引落し額Gを決済サーバ10へ送信する処理がなされる。決済サーバ10では、引落し額Gを受信すれば、VPの口座からGを減算してGを送信する処理がなされる（S89参照）。その結果、S210によりYESの判断がなされてS211へ進み、引落し額GをVP用IC端末19Vへ送信してGをリロード金額に加算更新する処理がなされる。

#### 【0307】

S196により、NOの判断がなされた場合には、図54（b）のS220へ進み、デビットカードの使用操作があったか否かの判断がなされる。デビットカードの使用操作があった場合には、S235へ進み、デビットカード使用要求を決済サーバ10へ送信する処理がなされる。次にS221へ進み、正当機関チェック処理（図50（a）参照）がなされる。そしてS222へ進み、 $R = DKP(L)$ であるか否かの判断がなされる。正当機関でない場合には、NOの判断がなされてS223へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合には制御がS224へ進み、デビットカードの暗証番号とカード情報の入力要求があったか否かの判断がなされ、あるまで待機する。決済サーバ10は、デビットカードの使用要求があった場合には、暗証番号とカード情報の入力要求をブラウザフォン30へ送信する（S70参照）。その送信を受信すれば、制御がS225へ進み、暗証番号の入力指示がブラウザフォン30の表示部76に表示される。ユーザがデビットカードの暗証番号をキーボードから入力すれば、S226によりYESの判断がなされてS227へ進み、VP用ICカード19Vからカード情報を読み出し暗証番号とともに決済サーバ10へ送信する処理がなされる。

#### 【0308】

次にS228へ進み、不適正である旨の返信があったか否かの判断がなされる。暗証番号とカード情報とを受信した決済サーバ10は、適正か否かの判断を行ない（S72）、適正でない場合には不適正である旨の返信を行なう（S79参照）。不適正である旨が返信されてくれば、S228によりYESの判断がなされてS229へ進み、不適正である旨の表示がなされる。一方、不適正である旨の返信が送られてこなければ、制御がS230へ進み、使用金額の入力指示がパーソナルコンピュータのディスプレイに表示される。ユーザが使用金額をキーボードから入力すれば、S231によりYESの判断がなされてS232へ進み、入力された使用金額Gを決済サーバ10へ送信する処理がなされる。

#### 【0309】

使用金額Gを受信した決済サーバ10は、前述したように、ユーザに該当する銀行口座を検索して使用金額Gを減算するとともに、その使用金額Gをブラウザフォン30に返信する処理を行なう（S74）。

#### 【0310】

その結果、S233によりYESの判断がなされてS234へ進み、決済が完了した旨



の表示をブラウザフォン30の表示部76に表示させる処理がなされる。

【0311】

S220によりNOの判断がなされた場合には、制御がS238へ進む。S238では、クレジットカードの使用操作があったか否かの判断がなされる。ユーザがブラウザフォン30のキーボード77を操作してクレジットカードの使用を入力すれば、制御がS237へ進み、クレジットカードによる決済要求を加盟店6へ送信する処理がなされる。この加盟店は、ユーザが商品やサービスを購入しようとしている商店である。次に制御がS239へ進み、正当機関チェック処理がなされる。この正当機関チェック処理は、図50(a)に示したものである。この正当機関チェック処理に合せて、加盟店6は、当該加盟店の電子証明書を顧客のブラウザフォン30へ送信し、次に乱数Rを受信すれば、その乱数を自己の秘密鍵K<sub>S</sub>を用いて暗号化し、その暗号結果Lを顧客のブラウザフォン30へ送信する。

【0312】

制御がS240へ進み、 $R = D_{KP}(L)$ であるか否かの判断がなされる。正当な販売店(加盟店)でない場合には、S240によりNOの判断がなされて、S241へ進み、正当な販売店でない旨の警告表示がなされる。一方、正当な販売店(加盟店)である場合には、S242へ進み、オーダ情報OIと支払指示PIとが作られる。オーダ情報OIとは、商品やサービス等の購入対象物や購入個数等を特定するための情報である。支払指示PIは、たとえばクレジットカード番号何々のクレジットカードを利用してクレジットの支払を行なう旨の指示等である。

【0313】

次にS243へ進み、オーダ情報OIと支払指示PIのメッセージダイジェストを連結した二重ダイジェストMDを算出する処理がなされる。次にS244へ進み、二重ダイジェストMDとクレジットカードを使用するVP氏名とをVP用IC端末19Vへ伝送して署名指示を出すとともに、VP用電子証明書の出力要求を行なう。

【0314】

クレジットカードを使用するVP氏名と署名指示と電子証明書の出力要求を受けたVP用IC端末19Vは、入力されたVP氏名をトラップ型RFID記憶領域と照合してそのVP氏名がVPの本名B13P(図9参照)を何回暗号化したものかを割出す。そしてその回数だけ秘密鍵を秘密鍵で暗号化して、その暗号化秘密鍵(K<sub>S</sub>)を用いて入力されたMDを復号化していわゆる二重署名を生成する。この二重署名を便宜上D<sub>(KS)</sub>(MD)と表現する。VP用IC端末19Vは、そのD<sub>(KS)</sub>(MD)をブラウザフォン30へ出力する。

【0315】

S244に従って入力されたVP氏名がVPの本名B13Pであった場合には、VP用IC端末19Vは、その本名に対する電子証明書を格納しているために、その格納している電子証明書をブラウザフォン30へ出力する。一方、S244に従って入力されたVP氏名がトラップ型VP氏名であった場合には、VP用IC端末19Vがそのトラップ型VP氏名用の電子証明書を格納していない。そのトラップ型VP氏名用の電子証明書は、前述したようにXMLストア50に格納されている。よって、その場合には、VP用IC端末19Vは、XMLストア50に電子証明書を取寄せる旨の指示をブラウザフォン30へ出力する。

【0316】

S244の要求をVP用IC端末19Vへ出力した後、VP用IC端末19Vから何らかの返信があれば、S245によりYESの判断がなされてS605へ制御が進む。S605では、XMLストア50への電子証明書の取り寄せ指示であったか否かの判断がなされ、取り寄せ指示でなかった場合にはS246へ進むが、取り寄せ指示であった場合には制御がS606へ進む。S606では、XMLストア50へアクセスしてトラップ型VP氏名に対応する電子証明書を検索してS246へ進み、オーダ情報OIと支払指示PIと出力されてきた署名としてのD<sub>(KS)</sub>(MD)とVP用電子証明書とを加盟店6へ送信する。

処理がなされる。加盟店 6 では、それら情報を確認した上で、ユーザの購入要求を受理する購入受理の回答をユーザのブラウザフォン 30 へ送信する。すると、S 247 により YES の判断がなされて S 248 へ進み、取引が完了した旨の表示が行なわれる。

#### 【0317】

S 238 により NO の判断がなされた場合に S 249 へ進み、リロード金額の使用操作があったか否かの判断がなされる。ユーザが、VP 用 IC 端末 19 V に蓄えられているリロード金額を使用する旨のキーボード操作を行なえば、制御が S 250 へ進み、使用金額の入力指示がブラウザフォン 30 のディスプレイに表示される。ユーザが使用金額をキーボードから入力すれば、S 251 により YES の判断がなされて S 252 へ進み、入力された使用金額 G の引落とし要求を VP 用 IC 端末 19 V へ伝送する処理がなされる。

#### 【0318】

VP 用 IC 端末 19 V では、後述するように、引落とし要求を受ければ、その使用金額 G だけリロード金額を減算更新し、引落としが完了した旨の信号をブラウザフォン 30 へ返信する。すると、S 252 a により YES の判断がなされて S 252 b へ進み、G の支払処理がなされる。

#### 【0319】

なお、RP 用決済処理は、以上説明した VP 用決済処理とほとんど同じ内容の処理であるために、図示および説明の繰返しを省略する。

#### 【0320】

図 56 は、図 27 に示した RFID 交換処理の他の例のサブルーチンプログラムを示すフローチャートである。図 56 の RFID 交換処理では、ブラウザフォン 30 により通話を行うことにより RFID の交換を行う。図 27 と同じ処理を行うステップには同じステップ番号を付してあり、ここでは主に相違点について説明する。SS1 により、ブラウザフォン 30 により通話を行ったか否かの判断がなされる。通話を行った場合には SE3 に進み、今日既に交換済みの相手（ブラウザフォン 30）でないことを条件に SE4 以降の RFID 交換処理を行う。

#### 【0321】

図 57 は、図 27 に示した RFID 交換処理のさらに他の例のサブルーチンプログラムを示すフローチャートである。図 57 の RFID 交換処理では、ブラウザフォン 30 により電子メールの送受信を行うことにより RFID の交換を行う。ST1 により Eメール（電子メール）の送信を行ったか否かの判断がなされる。行っていない場合には、ST2 へ進み、Eメールを受信したか否かの判断がなされる。受信していない場合には、このサブルーチンプログラムが終了する。

#### 【0322】

Eメールを送信する場合には、ST1 より YES の判断がなされ、SE3 により、今日既に RFID を交換済みの相手（ブラウザフォン 30）か否かの判断がなされる。既に交換済みの相手の場合には、このサブルーチンプログラムが終了する。交換済みでない場合には、SE4 へ進み、偽 RFID を記憶しているか否かの判断がなされる。ブラウザフォン 30 の EEPROM194 に偽 RFID を記憶しておれば、制御が ST3 へ進み、その記憶している偽 RFID を Eメールとともに相手のブラウザフォン 30 に発信する。一方、EEPROM194 に偽 RFID を全く記憶していない場合には、SE5 以降の偽 RFID を生成して相手に送信する処理がなされる。

#### 【0323】

Eメールを受信した場合には、ST8 へ進み、Eメールの相手から送られてきた偽 RFID を受信する。次に SE9 へ進み、EEPROM194 に既に記憶している偽 RFID を 1 つずつ古い記憶エリア側にシフトし、記憶上限を超えた 1 番古い偽 RFID を消去する処理がなされる。次に SE10 へ進み、1 番新しい記憶エリアに受信した偽 RFID を記憶する処理がなされる。

#### 【0324】

なお、図 56、図 57 に示した RFID 交換処理を、図 26 に示した RFID 交換処理

の代わりに用いるのではなく、図 26 に示した R F I D 交換処理にさらに付け加えて用いるようにしてもよい。また、個人ユーザがブラウザフォン 30 を操作して、図 26、図 56、図 57 の R F I D 交換処理の内の任意の 1 つまたは 2 つ以上のものを適宜選択して使用できるようにしてもよい。

#### 【0325】

ユーザがアクセスし自己の個人情報を提供した業者を特定するために用いる識別情報を特定可能な情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメール（Eメールやダイレクトメール）を送る場合には該メールに含まれることとなる識別情報として、前述した実施の形態では匿名（トラップ型 V P 氏名）を用いたが、その代わりにまたはそれに加えて、業者毎に使い分ける複数の Eメールアドレスやダイレクトメール用の住所（コンビニエンスストアの住所または私書箱等）を用いてもよい。すなわち、次のような個人情報保護装置であればよい。

#### 【0326】

コンピュータシステムを利用して、個人情報を保護する個人情報保護装置であって、ユーザが自己の個人情報を提供した業社を特定するために用いる識別情報を特定可能な情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメール（Eメール、ダイレクトメール）を送る場合には該メールに含まれることとなる識別情報を特定可能な情報（匿名としてのトラップ型 V P 氏名、図 44（a）の K S B とサイト名、サイト毎に使い分ける Eメールアドレスやダイレクトメール用の住所）を格納する識別情報格納手段（データベース 12 a，E E P R O M 26）と、前記個人情報を入手した者がその個人情報主であるユーザに対し送ったメール（Eメール、ダイレクトメール）に含まれている前記識別情報に基づいて特定される前記業社と前記メールの送り主とが一致するか否かを判定して前記ユーザの個人情報の流通状態を監視する監視手段（S 516，S 522，S 523）とを含む個人情報保護装置。

#### 【0327】

前述の実施の形態では、トラップ型 V P を利用しての個人情報の不正漏洩者と漏洩した個人情報の不正入手者との割出しを、トラップ型 V P の氏名を手掛かりに行なうものとした。そして、別実施の形態において、トラップ型 V P の Eメールアドレスをトラップ型 V P 毎に異ならせてもよい旨を示した。この別実施の形態のように、トラップ型 V P の氏名の代わりにトラップ型 V P の Eメールアドレスを利用し、前述の個人情報不正流出者と漏洩した個人情報の不正入手者との割出すようにしてもよい。即ち、トラップ型 V P 毎に異なる Eメールアドレスを登録しておき、トラップ型 V P 宛に Eメールが送信されて来た場合に、その Eメールの送信先である Eメールアドレスと一致するトラップ型 V P の Eメールアドレスを割出し、その割出された Eメールアドレスに対応する業社（トラップ型 V P の Eメールアドレスを通知した業社）を割出し、その割出された業社と Eメールを送信してきた送信元とが一致するか否かの整合性チェックを行ない、一致しない場合には前述の S 519～S 521 の異常時処理を行なう。

#### 【0328】

なお、このような Eメールアドレスの基づいた整合性チェックを行う場合には、トラップ型 V P に限定して行う必要がなく、R P が行うようにしてもよい。即ち、R P が自己の複数の Eメールアドレスを所有し、サイト（業社）毎に異なる Eメールアドレスを通知すると共にどの Eメールアドレスをどの業社に通知したかを V P 管理サーバ 9 または後述するメールサーバ 80 に登録しておき、送信されてきた Eメールの送信先の Eメールアドレスからその Eメールアドレスを通知した業社（サイト）を割出し、その割出された業社と Eメールの送信元とが一致するか否かの整合性チェックを行ない、個人情報の不正漏洩者や不正入手者を割出すようにしてもよい。

#### 【0329】

以下に、Eメールアドレスを利用した整合性チェックによる個人情報の不正流出者（不正漏洩者）と不正入手者との割出しを行う監視システムを説明する。

#### 【0330】

図58は、メールサーバ80およびそのデータベース81に記憶されているデータを示す図である。このメールサーバ80は、図1の広域・大容量中継網43やインターネット1や携帯電話網54等に接続されているものであり、ブラウザフォン30等のメールクライアントから送信されたEメールをその発信先Eメールアドレスに対応する送信先のメールボックスにまで送信して格納するためのものである。図58に示すように、データベース81には、鍵指定番号、共通鍵(KN)、Eメールアドレスの各データが記憶されるとともに、Eメールアドレスに対応するメールボックスが設けられている。共通鍵(KN)は、前述した認証鍵KNのことであるが、認証鍵KNに限らず、個人ユーザ(RPとVPの両者を含む)がメールサーバ80へ登録した共通鍵暗号方式用のEメール専用の鍵であってよい。

#### 【0331】

鍵指定番号は、そのメールサーバ80に登録されている共通鍵を指定するための番号である。この番号に従って登録されている複数の共通鍵のうちの対応する共通鍵が検索される。そのEメールアドレスは、メールサーバ80に登録されているユーザのEメールアドレスである。尚、あるユーザが複数のEメールアドレスをメールサーバ80に登録する場合もあり、その場合には、例えば、一つの鍵指定番号によってそのユーザの一つの共通鍵が特定されれば、その一つの共通鍵に対応するEメールアドレスが複数存在することとなる。

#### 【0332】

図59は、ブラウザフォン30によって行われるEメールアドレス通知処理のサブルーチンプログラムを示すフローチャートである。図59(b)は、IC端末19Rまたは19Vにより行われるEメールアドレス生成処理のサブルーチンプログラムを示すフローチャートである。

#### 【0333】

図59(a)を参照して、SU1により、Eメールアドレス生成操作があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。個人ユーザがブラウザフォン30を操作してEメールアドレス生成操作を行えば、SU1によりYESの判断がなされてSU2へ進み、Eメールアドレスを通知する相手特定する情報である通知相手特定情報を入力するメッセージ表示をブラウザフォン30により行う制御がなされる。この通知相手特定情報は、後述するように、通知相手の業社名と通知相手のEメールアドレスである。次にSU3により、通知相手特定情報の入力があったか否かの判断がなされ、あるまで待機する。個人ユーザがブラウザフォン30を操作して通知相手特定情報(通知相手の業社名と通知相手のEメールアドレス)を入力すれば、SU4へ進み、通知相手特定情報をブラウザフォン30に接続されているIC端末(19R又は19V)に入力する制御がなされる。

#### 【0334】

次にSU5により、接続されているIC端末から通知用Eメールアドレスが出力されて来たか否か判断され、出力されてくるまで待機する。出力されて来れば、SU6へ進み、その出力されて来た通知用Eメールアドレスをブラウザフォン30により表示させる制御を行う。そしてSU6aにより、その表示された通知用Eメールアドレスを通知相手に送信するための操作が行われたか否かの判断がなされる。通知用Eメールアドレスを通知する相手に対し、インターネットあるいはブルートゥース等の無線を使用して通知する場合には、その旨の操作をブラウザフォン30により行う。すると、制御がSU7へ進み、その通知用Eメールアドレスが通知相手に送信されることとなる。

#### 【0335】

図59(b)参照して、S1000により、通知相手特定情報がブラウザフォン30から入力されたか否かの判断がなされ、入力されていない場合には、このサブルーチンプログラムが終了する。入力された場合にはS1001へ進み、その入力された通知相手特定情報と個人ユーザのEメールアドレスとの両者を含むデータを共通鍵KNで暗号化する処理を行う。そしてS1002へ進み、その暗号結果のデータ中に鍵指定番号を分散挿入し

て通知用のEメールアドレスを生成する。そしてS103により、その生成された通知用のEメールアドレスをブラウザフォン30へ出力する処理を行う

ブラウザフォン30では、S1003により通知用Eメールアドレスが出力されて来れば、前述したようにSU5によりYESの判断がなされてSU16以降の処理を実行する

図60は、メールサーバ80の制御動作を示すフローチャートである。SV1によりEメールアドレスの登録要求があったか否かの判断がなされる。ない場合にはSV2へ進み、Eメールを受信したか否かの判断がなされ、受信していない場合にはSV3へ進み、その他の処理を行ってSV1へ戻る。このSV1→SV3をループの巡回途中で、ユーザからEメールアドレスの登録要求があった場合には、制御がSV4へ進み、そのユーザから送信されてきたEメールアドレスをデータベース80に登録する処理が行われる。その際に、当該ユーザの共通鍵やその共通鍵を指定するための鍵指定番号がデータベース80に未だ登録されていない場合には、メールサーバ80は、当該ユーザのための共通鍵とそれに対応する鍵指定番号とを生成してデータベース81に登録する。

#### 【0336】

次に、Eメールを受信すれば、SV2によりYESの判断がなされてSV5へ進み、その受信したEメールのEメールアドレス（SU7により送信した通知用Eメールアドレス）から鍵指定番号を抽出する処理が行われる。前述したように、通知用Eメールアドレスには、ユーザの鍵指定番号が分散挿入されており（S1002参照）、その分散挿入されている鍵指定番号をこのSV5により抽出するのである。次に制御がSV6に進み、その抽出された鍵指定番号に対応する共通鍵KNをデータベース81を検索して割出し、SV7により、受信した通知用Eメールアドレスから鍵指定番号を抽出した残りのデータをDPとしてそのDPをSV6により検索した共通鍵KNにより復号する演算を行なう。

#### 【0337】

次に、SV8により、メールヘッダ部分を読込み、SV9によりその読込んだメールヘッダ部分を解析し、SV10により受信Eメールの送信元の氏名とEメールアドレスとを抽出する。

#### 【0338】

次に、SV7による演算結果データの中の通知相手特定情報により特定される通知相手の業社名およびEメールアドレスとSV10により抽出された送信元（差出人）の氏名およびEメールアドレスとが一致するか否かを、S11によりチェックする処理が行われる。この一致判別は、受信したEメールに送信元（差出人）の氏名が示されておらず送信元（差出人）のEメールアドレスしか示されていなかった場合には、そのEメールアドレスとSV7による演算結果のデータ中の通知相手特定情報により特定されるEメールアドレスとが一致するか否かのみにより判断する。SV11によるチェックの結果、一致するか否かがSV12により判断され、一致する場合にはSV13に進み、演算結果データ中のEメールアドレスに相当するメールボックス（図58参照）に受信したEメールを格納する処理が行われる。

#### 【0339】

一方、SV11により、一致しないか判断された場合には、SV14へ進み、Eメールの受信元（差出人）に対応させて個人情報の不正入手値を「1」加算更新し、SV15により、特定された通知相手に対応させて個人情報の不正流出者の不正流出値を「1」加算更新し、SV16により演算結果データ中のEメールアドレスに相当するメールボックスに個人情報の漏洩レポートを格納する処理が行われる。個人ユーザは、自己のメールボックス中に格納された個人情報の漏洩レポートを呼出すことにより、個人情報の不正入手者、個人情報の不正流出者、送信されてきたEメールの内容等の詳しいレポートを閲覧することが出来る。また、メールサーバ80は、SV14、SV15の集計結果を公表する。なお、SV16の処理の代わりにまたはSV16の処理に加えて、個人情報の漏洩レポートを前述の個人情報の不正流出者宛さらには所定の個人情報保護機関（警察庁の担当部署等）に送信してもよい。

#### 【0340】

さらに、前述のSG13により予め選択指定されている業者に対応するRFIDを発信した場合に、その予め選択指定されている業者名とRFIDを発信した発信先の業者名とを対応付けてブラウザフォン30等に記憶しておくとともに、メールサーバ80等にも予め選択指定されている業者名とRFIDを発信した発信先の業者名とを送信して、両者を対応付けて記憶させるようにしてもよい。このようにすれば、個人情報の不正入手者と個人情報の不正流出者が、予め選択指定されている業者名とRFIDを発信した発信先の業者名の記憶情報に一致したときには、前述の個人情報の不正入手者がSG13により発信されたトラップ型RFIDを悪用して個人情報を不正に入手した者である疑いが高くなる。

#### 【0341】

図61は、図59、図60に示した制御内容を分かり易く説明するための説明図である。まず、個人ユーザが顧客またはユーザとして業社に自己のEメールアドレスを通知する際には、個人ユーザ側端末としてのブラウザフォン30にIC端末19を取付けて通知用のEメールアドレスを生成する。IC端末19は、個人ユーザがVPとしてEメールアドレスを通知する場合にはVP用IC端末19Vを用い、個人ユーザがRPとしてEメールアドレスを通知する場合にはRP用IC端末19Rを用いる。通知用Eメールアドレスを生成するには、まず、業社側端末82から通知相手の業社の業社名MTTとEメールアドレス〇△××△とからなる通知相手特定情報MTT//〇△××△を送信してもらう。その通知相手特定情報を受信したブラウザフォン30およびIC端末19において、前述したように、受信した通知相手特定情報(MTT//〇△××△)と個人ユーザ(VPまたはRP)のEメールアドレス(〇□×△×)とを個人ユーザの共通鍵KNIにより暗号化、すなわち $E_{KNI}(MTT//〇△××△//〇□×△×)$ を演算して、 $\#e\forall 8\%3\&\alpha t*c$ を生成する。この暗号データに予め決められたフォーマットに従って鍵指定番号(92103)を分散挿入する。この実施の形態の場合、左から数えて、2番目と3番目の間、4番目と5番目の間、6番目と7番目の間、7番目と8番目の間、8番目と9番目の間に、鍵指定番号(92103)の各数値を1つずつ分散挿入する。そして出来上がった $\#e\forall 8\%3\&0\alpha 3 t*c$ を、通知用Eメールアドレスとして業社側端末82へ送信する。

#### 【0342】

以降、業社側は、 $\#e\forall 8\%3\&0\alpha 3 t*c$ をEメールアドレスとして個人ユーザにEメールを送ることとなる。業社MTTが業社側端末82によりEメール85を作成し、送信先Eメールアドレスを $\#e\forall 8\%3\&0\alpha 3 t*c$ としてEメール85を送信すれば、そのEメール85がメールサーバ80に送られる。メールサーバ80では、前述の鍵指定番号の挿入フォーマットに従って、Eメール85の送信先Eメールアドレス $\#e\forall 8\%3\&0\alpha 3 t*c$ 中に分散挿入されている鍵指定番号を抽出する。その抽出した鍵指定番号92103に基づいてデータベース81を検索して対応する鍵KNIを割出す。次に、送信先Eメールアドレスから鍵指定番号を抜き去った残りのデータ $\#e\forall 8\%3\&\alpha t*c$ を前述の割出された共通鍵KNIで復号する演算、すなわち $D_{KNI}(\#e\forall 8\%3\&\alpha t*c)$ を行ない、 $MTT//〇△××△//〇□×△×$ を算出する。この算出データ中のMTT//〇△××△が通知相手特定情報であり、本来なら、受信Eメール85の送信元の名前とEメールアドレスに一致するはずである。この通知相手特定情報であるMTT//〇△××△と受信Eメール85の送信元の名前およびEメールアドレスとを比較し、一致しておれば、算出したMTT//〇△××△//〇□×△×中の送信先Eメールアドレスである〇□×△×に相当するメールボックスに受信Eメールを格納する。その結果個人ユーザが自分のメールボックスにアクセスして受信Eメールをダウンロードして閲覧可能となる。

#### 【0343】

一方、通知相手特定情報であるMTT//〇△××△と受信Eメール85の送信元の名前およびEメールアドレスとを比較し、一致していなければ(たとえば、送信元の名前がMEC等の場合)、通知相手業者MTTから個人ユーザのEメールアドレスを含む個人情報



が漏洩され、その漏洩されたEメールアドレスを不正入手した者（たとえば、MEC）がそのEメールアドレス宛にEメールを送信してきたことが想定されるため、前述のSV14～SV16の異常時処理を行なう。

#### 【0344】

以上の監視システムでは、個人情報の不正入手者（たとえば、MEC）が自己の業社名やEメールアドレスを使用することな個人情報の不正流出者の業社名（たとえば、MTT）やEメールアドレスを使用してEメールを送信した場合には、不正の監視ができない。しかし、個人情報の不正入手者（たとえば、MEC）は、たとえば自社製品の売込みや宣伝等の営業活動の一環としてEメールを送信するのであり、Eメールの送信元として他社の業社名（たとえば、MTT）やEメールアドレスを使用したのでは、自社製品の売込みや宣伝等の営業活動にはならない。よって、個人情報の不正入手者の営業活動としてのEメールの送信に対しては、有効な監視システムである。

#### 【0345】

なお、前述の通知相手特定情報であるMTT//○△××△と受信Eメール85の送信元の名前およびEメールアドレスとの比較判定は、完全に一致するか否かにより判定してもよいが、少なくともEメールアドレスが一致していれば適正と判定してもよい。また、受信Eメールに含まれている送信元特定情報として、送信者名と送信元Eメールアドレスとのいずれか一方しかない場合がある。その場合は、そのいずれか一方の送信元特定情報と通知相手特定情報とが一致すれば適正であると判定してもよい。さらに、通知相手特定情報を通知相手のEメールアドレスのみにしてもよい。

#### 【0346】

以上説明したEメールアドレスを利用した整合性チェックによる個人情報の不正流出者（不正漏洩者）と不正入手者との割出しを行なう監視システムは、Eメールの受取り側のみが暗号化Eメールアドレスを採用している場合を示した。次に、Eメールの受取り側と送信側との双方が暗号化Eメールアドレスを採用している場合を説明する。まず、双方が互いのEメールアドレス○□×△×、○△××△を送信し、受信した相手のEメールアドレスを用いて前述と同様の方法で通知用Eメールアドレスを生成して相手に返信して通知する。業者MTTが個人ユーザにEメールを送るときには、前述と同様に、送信先Eメールアドレスとして#e9¥82%31&0α3t\*c、送信元の名前としてMTT、送信元Eメールアドレスとして○△××△のEメール85を作成して送信する。メールサーバ80での整合性チェックも前述と同様の方法で行なう。

#### 【0347】

なお、Eメール85を受信した個人ユーザがEメールを返信するときには、Eメール85に示されている送信元のEメールアドレス○△××△に返信したのでは業者MTTに届かない。業者MTTから通知してもらった通知用Eメールアドレス、すなわち個人ユーザ名と個人ユーザのEメールアドレス○□×△×とを業者の共通鍵（たとえばKN1）で暗号化したデータに鍵指定番号を分散挿入して生成された通知用Eメールアドレス宛に、Eメールを返信しなければならない。これを可能にするため、個人ユーザのブラウザフォン30は、業者MTTから通知された通知用Eメールアドレスと業者MTTのEメールアドレス○△××△とを対応付けて記憶しており、Eメールアドレス○△××△を入力することによって業者MTTの通知用Eメールアドレスを検索して出力できるように構成されている。業者MTTの端末82も同様に、個人ユーザから通知された通知用Eメールアドレスと個人ユーザのEメールアドレス○□×△×とを対応付けて記憶しており、Eメールアドレス○□×△×を入力することによって個人ユーザの通知用Eメールアドレスを検索して出力できるように構成されている。

#### 【0348】

このような、送信されてきたEメールの送信元Eメールアドレスをそのまま使用してEメールの返信ができない不都合を解消する方法として、次のような変形システムを採用してもよい。互いにEメールアドレスを交換して相手のEメールアドレスを用いて通知用Eメールアドレスを生成して返信し、Eメール85を相手の通知用Eメールアドレス宛に送



信する点は、前述と同じであるが、Eメール85の送信元のEメールアドレスを相手に通知した送信元の通知用Eメールアドレスにする。これにより、Eメール85を受信した者は、そのEメール85に示されている送信元の通知用Eメールアドレス宛にそのままEメールを返信すれば、そのEメールが送信元に届く。そして、メールサーバ80において、送信されてきたEメール85の送信先Eメールアドレス#e9¥82%31&0α3t\*cから算出された通知相手特定情報中のEメールアドレス○△××△とEメール85に示されているの送信元の通知用Eメールアドレスとを直接比較するのではなく、通知用Eメールアドレスを前述の演算手順に従って復号してEメールアドレス○△××△を算出し、その算出されたEメールアドレスと送信先Eメールアドレスから算出された通知相手特定情報中のEメールアドレスとを比較判定する。

#### 【0349】

また、通知用Eメールアドレス（たとえば#e9¥82%31&0α3t\*c）を、通常のEメールアドレス（たとえば○□×△×）に比べて一見区別がつかない記号の組合せで構成するようにしてもよい。これにより、個人情報の不正入手者が、不正入手した個人情報中の通知用Eメールアドレスを通常のEメールアドレスと思い、なんら疑うことなく通知用Eメールアドレス宛にEメールを送信することとなり、畏にかかり易くなる利点がある。

#### 【0350】

さらに、暗号化して通知用Eメールアドレスを生成するのに代えて、通知相手毎に専用のEメールアドレスを生成して、該専用Eメールアドレスとそれに対応する通知相手とを対応付けてメールサーバ80およびブラウザフォン30等に登録しておくようにしてもよい。そして、送信されてきたEメールの送信先Eメールアドレスである専用Eメールアドレスに対応する通知相手を登録されている通知相手から検索して割出し、その割出された通知相手と送信されて来たEメールの送信元とが一致するか否かの整合性チェックを行う。なお、この発明における「暗号化」とは、所定のアルゴリズムに従ってデータを変換するのも全てを含む広い概念である。また、「復号」とは、暗号化されたデータを所定のアルゴリズムに従って元のデータに戻すもの全てを含む広い概念である。

#### 【0351】

以上説明した、個人情報の不正流出者（不正漏洩者）と不正入手者との割出しを行なう監視システムは、自己のメールアドレス（通知用Eメールアドレス）を自ら通知した相手以外の者からのEメールの受信を防止でき、迷惑メール（スパム）を有効に防止できる利点も有している。また、個人ユーザと業者との間でEメールを送受信するものを示したが、それに限らず、個人ユーザ同士間または業者同士間でEメールを送受信するものであってもよい。以下に、個人情報の不正流出者（不正漏洩者）と不正入手者との割出しを行なう監視システム、および、迷惑メール（スパム）の監視システムの発明を、まとめて説明する。

#### 【0352】

従来から、個人情報の漏洩を防止する技術は多数存在しているが、一旦個人情報が漏洩した場合に、どこの業者等から漏洩したのかという漏洩主体を割出すために有効な技術は存在しなかった。さらに、その漏洩した個人情報を不正に入手した者を突き止めるために有効な技術は存在しなかった。また、迷惑メール（スパム）が送信されてきた場合に、その迷惑メール（スパム）の送信元や送信経路等をメールサーバ等に登録して、次回から同じ送信元や送信経路等を介して送信されてくる迷惑メール（スパム）を防止する技術があった。しかし、登録する前すなわち初回の迷惑メール（スパム）の着信を防止できず、かつ、ユーザがわざわざ迷惑メール（スパム）の送信元や送信経路等をメールサーバ等に登録しなければならず、面倒であった。

#### 【0353】

この監視システムの発明の目的は、個人情報の漏洩主体を割出すことを可能にすることである。また、漏洩した個人情報を不正に入手した者を突き止めることを可能にすることである。また、初回の迷惑メール（スパム）の着信を防止でき、かつ、迷惑メール（スパ

ム)の送信元や送信経路等をメールサーバ等に登録する煩雑な作業をユーザに強いることなく迷惑メール(スパム)の着信を防止することである。

#### 【0354】

このよな目的を達成するべく、この監視システムの発明は、次のような手段を採用する。なお、各手段の具体例を括弧書きで挿入して示す。

#### 【0355】

(1) 個人情報の漏洩を監視する監視システムであって、

相手に自己のメールアドレスを通知するときの通知用メールアドレスを生成する手段であって、通知相手を特定する情報を割出すことが可能な通知用メールアドレス(たとえば、図61の#e9¥82%31&0α3t\*c)を生成するための処理を行う通知用メールアドレス生成処理手段(たとえば、図59のS1000~S1003)と、

送信元(たとえば、図61のMTT)から送信された電子メール(たとえば、図61のEメール85)の送信先のメールアドレスが、前記通知用メールアドレス生成処理手段により生成された前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知相手を特定する情報(たとえば、図61のMTT//○△××△)を割出し、該割出された通知相手を特定する情報と当該電子メールの送信元の情報とが一致するか否かを監視する監視手段(たとえば、図60のSV5~SV16)を含むことを特徴とする、監視システム。

#### 【0356】

このような構成によれば、通知相手に通知した通知用メールアドレスの個人情報が漏洩されて、その個人情報を不正入手した者がその個人情報としての通知用メールアドレス宛に電子メールを送信した場合に、当該電子メールの通知用メールアドレスから割出される通知相手を特定する情報と当該電子メールの送信元の情報とを比較することにより両者が一致しないことが判明でき、割出された通知相手から個人情報が漏洩した可能性が高いことと、その漏洩した個人情報を当該電子メールの送信元が不正入手した可能性が高いことを、突き止めることができる。

#### 【0357】

(2) 前記通知用メールアドレス生成処理手段は、前記通知相手を特定するための通知相手特定情報(たとえば、図61のMTT//○△××△)を含むデータを暗号化して前記通知用メールアドレスを生成するための処理を行い(たとえば、図59のS1001により暗号化してS1002により鍵指定番号を分散挿入して生成し)、

前記監視手段は、前記通知用メールアドレスを復号して(たとえば、図60のSV5、SV6により共通鍵KNを割出し、SV7により鍵KNを用いて復号する)前記通知相手特定情報を抽出し、該通知相手特定情報と前記電子メールの送信元の情報とが一致するか否かを監視する(たとえば、図60のSV8~SV12)ことを特徴とする、(1)に記載の監視システム。

#### 【0358】

このような構成によれば、通知用メールアドレスのデータ自体から通知相手特定情報を割出すことができ、たとえば通知用メールアドレス毎に対応する通知相手特定情報を登録しておく方法に比べて、多数の相手にそれぞれ通知用メールアドレスを通知した場合の通知相手特定情報の登録データ量が膨大になる不都合を防止できる。

#### 【0359】

(3) 前記通知用メールアドレス生成処理手段は、前記通知相手に通知した本人のメールアドレス(たとえば、図61の○□×△×)を含むデータを暗号化して前記通知用メールアドレスを生成する処理を行い、

前記監視手段は、前記通知用メールアドレスを復号して前記通知相手に通知した本人のメールアドレスを抽出し、監視結果適正な電子メールの場合に前記抽出した本人のメールアドレスに対応するメールボックスに当該電子メールを格納する(たとえば、図60のSV13)ことを特徴とする、(2)に記載の監視システム。

#### 【0360】

このような構成によれば、監視のために通知用メールアドレスを復号することにより、本人のメールアドレスも抽出でき、利便性が向上する。

**【0361】**

(4) 迷惑メールを監視して防止するための監視システムであって、相手に自己のメールアドレスを通知するときの通知用メールアドレスを生成する手段であって、通知相手を特定する情報を割出すことが可能な通知用メールアドレス（たとえば、図61の#e9¥82%31&0α3t\*c）を生成するための処理を行う通知用メールアドレス生成処理手段（たとえば、図59のS1000～S1003）と、

送信元（たとえば、図61のMTT）から送信された電子メール（たとえば、図61のEメール85）の送信先のメールアドレスが、前記通知用メールアドレス生成処理手段により生成された前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知相手を特定する情報（たとえば、図61のMTT//○△××△）を割出し、該割出された通知相手を特定する情報と当該電子メールの送信元の情報とが一致するかどうか監視する監視手段（たとえば、図60のSV5～SV16）とを含むことを特徴とする、監視システム。

**【0362】**

このような構成によれば、通知用メールアドレスを通知した通知相手以外の者がその通知用メールアドレス宛に電子メールを送信した場合に、当該電子メールの通知用メールアドレスから割出される通知相手を特定する情報と当該電子メールの送信元の情報とを比較することにより両者が一致しないことが判明でき、その不適正な電子メールの送信を阻止することができる。

**【0363】**

(5) 前記通知用メールアドレス生成処理手段は、前記通知相手を特定するための通知相手特定情報（たとえば、図61のMTT//○△××△）を含むデータを暗号化して前記通知用メールアドレスを生成するための処理を行い（たとえば、図59のS1001により暗号化してS1002により鍵指定番号を分散挿入して生成し）、

前記監視手段は、前記通知用メールアドレスを復号して（たとえば、図60のSV5、SV6により共通鍵KNを割出し、SV7により鍵KNを用いて復号する）前記通知相手特定情報を抽出し、該通知相手特定情報と前記電子メールの送信元の情報とが一致するかどうか監視する（たとえば、図60のSV8～SV12）ことを特徴とする、(4)に記載の監視システム。

**【0364】**

このような構成によれば、通知用メールアドレスのデータ自体から通知相手特定情報を割出すことができ、たとえば通知用メールアドレス毎に対応する通知相手特定情報を登録しておく方法に比べて、多数の相手にそれぞれ通知用メールアドレスを通知した場合の通知相手特定情報の登録データ量が膨大になる不都合を防止できる。

**【0365】**

(6) 前記通知用メールアドレス生成処理手段は、前記通知相手に通知した本人のメールアドレス（たとえば、図61の○□×△×）を含むデータを暗号化して前記通知用メールアドレスを生成する処理を行い、

前記監視手段は、前記通知用メールアドレスを復号して前記通知相手に通知した本人のメールアドレスを抽出し、監視結果適正な電子メールの場合に前記抽出した本人のメールアドレスに対応するメールボックスに当該電子メールを格納する（たとえば、図60のSV13）ことを特徴とする、(5)に記載の監視システム。

**【0366】**

このような構成によれば、監視のために通知用メールアドレスを復号することにより、本人のメールアドレスも抽出でき、利便性が向上する。

**【0367】**

(7) 前記監視手段による監視の結果、前記割出された通知相手特定情報と当該電子メールの送信元の情報とが一致しない場合に（たとえば、図60のSV12によりNOの

判断がなされた場合に)、当該電子メールの送信を阻止する阻止手段(たとえば、図60のSV14~SV16)をさらに含むことを特徴とする、(4)~(6)のいずれかに記載の監視システム。

【0368】

このような構成によれば、阻止手段によって迷惑メールの着信を確実に防止できる。

【0369】

次に、以上説明した実施の形態における変形例や特徴点等を以下に列挙する。

【0370】

(1) 本発明でいう「人物」の用語は、自然人に限らず法人をも含む広い概念である。本発明でいう「匿名」とは、仮想人物(VP)の氏名のことであり、仮想人物の氏名と実在人物の匿名とは同じ概念である。したがって、仮想人物の住所やEメールアドレスや電子証明書は、実在人物が匿名でネットワーク上で行動する場合の住所、Eメールアドレス、電子証明書ということになる。

【0371】

本発明でいう「個人情報保護装置」は、装置単体ばかりでなく、複数の装置がある目的を達成するために協働するように構築されたシステムをも含む広い概念である。

【0372】

(2) 図1に示すように、本実施の形態では、金融機関7に、VP管理機能と、決済機能と、認証機能とを設けたが、金融機関7から、VP管理機能を分離独立させ、金融機関以外の他の守秘義務を有する所定機関にVP管理機能を肩代わりさせてもよい。その肩代わりする所定機関としては、官公庁等の公共的機関であってもよい。さらに、RPやVPに電子証明書を発行する電子証明書発行機能を、金融機関7から分離独立させ、専門の認証局に肩代わりさせてもよい。

【0373】

また、本実施の形態では、コンビニエンスストア2の住所をVPの住所としているが、その代わりに、たとえば郵便局や物流業者における荷物の集配場等をVPの住所としてもよい。またVPの住所となる専用の施設を新たに設置してもよい。

【0374】

VPを誕生させる処理は、本実施の形態では、所定機関の一例としての金融機関7が行なっているが、本発明はこれに限らず、たとえば、ユーザ自身が自己の端末(ブラウザフォン30等)によりVPを誕生(出生)させ、その誕生させたVPの氏名、住所、公開鍵、口座番号、Eメールアドレス等のVP用情報を、金融機関7等の所定機関に登録するようにしてもよい。

【0375】

また、誕生したVPは、必ずしも所定機関に登録させなくてもよい。

【0376】

(3) 処理装置の一例としてのIC端末19Rまたは19Vは、ICカードや携帯電話あるいはPHSやPDA(Personal Digital Assistant)等の携帯型端末で構成してもよい。これら携帯型端末で構成する場合には、VP用の携帯型端末とRP用の携帯型端末との2種類のものを用意してもよいが、VP用モードあるいはRP用モードに切換え可能に構成し、1種類の携帯型端末で事足りるように構成してもよい。

【0377】

図7に示したIC端末19Iによるアプリケーションソフトのインストールに代えて、当該アプリケーションソフトのサプライヤからネットワーク経由で当該アプリケーションソフトをブラウザフォン30等へダウンロードするように構成してもよい。

【0378】

(4) 本実施の形態では、図17に示したように、VPの誕生時にそのVPの電子証明書が自動的に作なされて発行されるように構成したが、その代わりに、ユーザからの電子証明書の発行依頼があつて初めてVPの電子証明書の作成発行を行なうようにしてもよい。

## 【0379】

図23等に示すように、本実施の形態では、RPの本人認証を行なう場合には、RPの認証鍵KNを用いるようにしたが、RPが電子証明書の発行を受けている場合には、その電子証明書内の公開鍵を用いてRPの本人認証を行なうようにしてもよい。

## 【0380】

(5) ブラウザフォン30に代えて、パーソナルコンピュータを用いてもよい。

## 【0381】

トラップ型VP用に金融機関7が開設したEメールアドレス△△△△△は、1種類のためのEメールアドレスではなく、複数種類用意し、トラップ型VP氏名毎に使い分けるようにしてもよい。S620～S622またはS960～S956により、新たな匿名（トラップ型VP氏名）の生成要求があった場合に、今までに使われていない匿名を生成する新匿名生成手段が構成されている。S431～S441またはS954により、前記新匿名生成手段により生成された匿名の登録を行なう匿名登録機関（金融機関7またはEEROM26）に対し新たに生成された匿名の登録依頼があった場合に、該匿名を登録する匿名登録手段が構成されている。

## 【0382】

前述したS450～S460により、ユーザの個人情報を登録している登録機関に対しユーザから自己の個人情報の確認要求があった場合に、当該ユーザの本人認証を行なう本人認証手段（S452～S458）による本人認証の結果本人であることが確認されたことを条件として、当該ユーザに対応する個人情報を当該ユーザに送信する個人情報送信手段が構成されている。

## 【0383】

図40(a)で示したトラップ型VP氏名は、サイト名（業社名）をVPの秘密鍵KSBで復号化したものであってもよい。

## 【0384】

つまり、S957により、DKSB（業社名）の演算を行なってトラップ型VP氏名を生成してもよい。その場合には、S969により、EKPB（Eメールの宛名）＝送信者名の演算式による判別を行なうこととなる。S967では、EKPB（Eメールの宛名）が不正流出し、送信者名の業者が不正入手した旨を出力するという処理になる。

## 【0385】

(6) 前述した正当機関証明処理、正当機関チェック処理、本人証明処理、S4～S7等の本人チェック処理により、本人であることの確認を行なってなりすましを防止するための本人認証手段が構成されている。

## 【0386】

S13～S16により、バーチャルパーソン（仮想人物）用の電子証明書を作成して発行する仮想人物用電子証明書発行手段が構成されている。S25～S28により、現実世界に実在するリアルパーソン（実在人物）用の電子証明書を作成して発行する実在人物用電子証明書発行手段が構成されている。

## 【0387】

S39～S45により、仮想人物（バーチャルパーソン）用の銀行口座を作成するための処理を行なう銀行口座作成処理手段が構成されている。

## 【0388】

S40～S49により、実在人物（リアルパーソン）または仮想人物（バーチャルパーソン）用のデビットカードを発行するための処理を行なうデビットカード発行処理手段が構成されている。S55～S69により、仮想人物（バーチャルパーソン）に携帯される処理装置（VP用IC端末19V）に対し、該仮想人物（バーチャルパーソン）の銀行口座内の資金の一部を引落してリロードするための処理を行なう資金引落し処理手段が構成されている。

## 【0389】

S57～S74により、仮想人物（バーチャルパーソン）のデビットカードを使用して

決済を行なうための処理を行なうデビットカード用決済処理手段が構成されている。S 5 7 ~ S 7 8 により、仮想人物（バーチャルパーソン）のクレジットカードを使用しての決済を行なうための処理を行なうクレジットカード用決済処理手段が構成されている。このクレジットカード用決済処理手段は、Secure Electronic Transaction (S E T) に準拠して決済を行なう。

#### 【0390】

(7) S 1 4 0 ~ S 1 5 8 により、ユーザが自己の仮想人物（バーチャルパーソン）の出生依頼を行なう処理を行なうための出生依頼処理手段が構成されている。S 9 ~ S 1 2 により、出生させる仮想人物（バーチャルパーソン）の住所であって出生依頼者である実在人物（リアルパーソン）の住所とは異なった住所を決定するための処理を行なう住所決定処理手段が構成されている。この住所決定処理手段は、コンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定する。また、この住所決定処理手段は、出生依頼者である実在人物（リアルパーソン）の希望するコンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定可能である。また、この住所決定処理手段は、出生依頼者である実在人物（リアルパーソン）の住所に近いコンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定することが可能である。

#### 【0391】

S 3 0 5 ~ S 3 1 2 により、ユーザに携帯される前記処理装置（R P 用 I C 端末 1 9 R , V P 用 I C 端末 1 9 V）に設けられ、当該処理装置の所有者であるユーザの実在人物（リアルパーソン）としての個人情報または仮想人物（バーチャルパーソン）としての個人情報の送信要求を受けた場合に、記憶している個人情報の中から該当する個人情報を選び出して出力する処理が可能な個人情報自動出力手段が構成されている。この個人情報自動出力手段は、送信要求の対象となっている個人情報が送信してよいものであるか否かを自動的に判別するための処理を行なう自動判別処理手段（S 3 0 7 , S 3 0 8 , S 3 1 0 , S 3 1 1）を含んでいる。この自動判別処理手段は、どの種類の個人情報を出力してよいかをユーザが事前に入力設定でき、その入力設定に従って自動判別を行なう。またこの自動判別処理手段は、自動判別できない場合には、要求対象となっている個人情報と送信されてきたプライバシーポリシーとを出力してユーザに対し送信の許否を求めるための処理を行なう（S 3 0 9）。

#### 【0392】

コンビニエンスストア 2 により、仮想人物（バーチャルパーソン）がネットワーク上で購入した商品が配達されてきた場合に当該商品を預る商品預り場が構成されている。データベース 1 7 により、前記商品預り場で商品を預る対象となる仮想人物（バーチャルパーソン）を登録しておくバーチャルパーソン登録手段が構成されている。このバーチャルパーソン登録手段は、仮想人物（バーチャルパーソン）ごとに分類して、商品を預っているか否かを特定するための預り特定情報が記憶される。さらに、当該商品の決済が済んでいるか否かを特定するための決済特定情報が記憶される。また、前記仮想人物（バーチャルパーソン）ごとに分類して当該仮想人物（バーチャルパーソン）の E メールアドレスを記憶している。

#### 【0393】

S 3 2 3 により、前記商品預り場に設けられ、商品を預っている仮想人物（バーチャルパーソン）の E メールアドレスに対し商品を預った旨の E メールを送信するための処理を行なう E メール送信処理手段が構成されている。S 3 1 7 ~ S 3 4 0 により、前記商品預り場に設けられ、ユーザが仮想人物（バーチャルパーソン）として商品を引取りにきた場合に、当該ユーザに対し該当する商品を引渡すための処理を行なう商品引渡し処理手段が構成されている。この商品引渡し処理手段は、引取りにきたユーザの仮想人物（バーチャルパーソン）が本人であることを確認できたことを条件として引渡し処理を行なう。前記商品引き渡し処理手段は、引き渡す商品が決済済みであるか否かを判別し、決済済みでない場合には決済が行なわれたことを条件として商品の引渡し処理を行なう。



## 【0394】

(8) 前記ライフ支援センター8のサービス提供サーバ13により、ユーザの個人情報を収集して、該個人情報に基づいて当該ユーザのライフを支援するライフ支援手段が構成されている。このライフ支援手段は、ユーザの人生の根幹をなす上位の事項（たとえばユーザの夢や人生設計）を推薦し、次にそれよりも下位の事項（たとえば職種や進路等）を推薦し、次にさらに下位の事項（たとえば趣味等）を推薦する等のように、上位から下位への順に推薦処理を行なう。さらに、ライフ支援処理手段は、推薦した事項に関連する消費支援業者（ニューミドルマン等の加盟店）を推薦する処理を行なう。その推薦の際に、収集した当該ユーザの個人情報を前記推薦した消費支援業者に提供する。

## 【0395】

(9) 可変型偽識別子生成手段（図26のSD10、図27のSE1～SE10、図29のSG6～SG9、図56のRFID交換処理、図57のRFID交換処理等）は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置（RFIDタグ）の各々が発信する識別子の範囲内で偽識別子（偽RFID等）を生成する。また、図12に示した、共通偽識別子（共通偽RFID等）を生成する機能および所定個数（たとえば1個）の偽識別子（偽RFID等）と当該所定個数よりも多い個数の偽識別子（偽RFID等）を生成する機能を、ブラウザフォン30にも備えてもよい。

## 【0396】

(10) セキュリティ用の識別子発信装置を、指輪等の形状をした携帯装置（IDリング）1として個人ユーザに提供（販売）する代わりに、RFIDタグ1aの状態でも個人ユーザに提供（販売）してもよい。その場合には、個人ユーザ自身が自己の携帯品等にRFIDタグ1aを貼着する。

## 【0397】

(11) 図10のコンデンサ110により、外部からの電源用電波を受信して動作可能となるセキュリティ用の識別子発信装置に備えられ、受信した電源用電波によって発生した電力を貯える蓄電気手段が構成されている。図11のSA6～SA10aにより、外部からの電源用電波が途絶えた後においても、前記蓄電気手段から供給される電力を利用して数値データを更新する数値データ更新手段が構成されている。換言すれば、図11のSA6～SA10aにより、外部からの電源用電波が途絶えた後においても、前記蓄電気手段から供給される電力を利用して乱数を生成する乱数生成手段が構成されている。図11のSA4により、前記数値データ更新手段から抽出された数値データを用いて偽識別子を生成する偽識別子生成手段が構成されている。換言すれば、図11のSA4により、前記乱数生成手段により生成された乱数を用いて偽識別子を生成する偽識別子生成手段が構成されている。蓄電気手段に蓄電される電力量が毎回不規則のために蓄電気手段の放電期間も不規則となり、その不規則な期間を利用して生成されたランダムな数値データ（乱数）を用いて偽識別子が生成されるため、ランダムな偽識別子を生成することができる。

## 【0398】

識別子を記憶する識別子記憶手段（図27、図56、図57のSE9、SE10とEEPROM194等）は、交換された偽識別子を複数記憶可能である。また、交換された偽識別子とその交換順に複数記憶可能であり、上限個数の偽識別子を記憶している状態で識別子の交換が行われることにより、記憶中の最も古い偽識別子を消去する（SE9）。図29のSG9により、前記識別子記憶手段に記憶されている複数の偽識別子から発信する偽識別子を選択する手段であって、前回選択した偽識別子とは異なる偽識別子を選択可能な偽識別子選択手段が構成されている。図29のSG2により、識別子の送信要求があった場合にその旨を報知する識別子送信要求報知手段が構成されている。

## 【0399】

(12) 図41～図47に基づいて説明したように、購入商品に付されている固有の識別子発信装置（RFIDタグ）から発信される固有の識別子（RFID）を利用して、当該商品に関連する種々の情報が個人ユーザに提供される。この情報提供システムは、商品メーカー300のサーバとデータベース、商品情報サービス業者302のサーバとデー



データベース、中間流通業者301のサーバとデータベース、小売店20bとからなる商品販売店のサーバとデータベースと、それらサーバ間で通信を行う通信網（広域・大容量中継網43）から構成される。

#### 【0400】

商品情報サービス業者302のデータベースには、図42に示すような、固有の識別子（RFID）のそれぞれに対応させて、生産者、中間流通業者、小売店の各URLが記憶されている。さらに、購入した商品に付されている固有の識別子発信装置（RFIDタグ）から発信される固有の識別子（RFID）に対応させて当該商品を購入した購入者の情報が記憶可能に構成されている。購入者が固有の識別情報（RFID）を商品情報サービス業者302のサーバへ送信してそのサーバにアクセスすることにより、送信した固有の識別情報に対応して当該購入者の情報記録領域（購入者ページ）が設けられる。その情報記録領域（購入者ページ）に、購入者の匿名（VP名）やVP住所やEメールアドレス等を記録することができるよう構成されている。またその購入者ページに、購入者が、購入商品に関するメモ書き等を書込むことができるように構成されており、購入者は商品に関する種々の情報を書込んで、固有の識別情報（RFID）を商品情報サービス業者302のサーバへ送信してそれに対応する書込み情報を検索して閲覧できるように構成されている。

#### 【0401】

図46のSQ26により、購入したい商品を当該商品に対応する固有の識別情報により特定して小売店に送信して購入予約を行う購入予約手段が構成されている。図46のSQ33、SQ35により、個人ユーザ同士で物々交換を行う物々交換手段が構成されている。図46のSQ34により、個人ユーザが自己所有の中古商品を販売するための中古商品販売手段が構成されている。図47のSS3～SS12により、個人ユーザからの予約購入を受付けて処理するための予約購入受付処理手段が構成されている。なお、本発明でいう「識別子」とは、RFIDに限るものではなく、それを基にプライバシーが侵害される虞の有る識別子であれば全て含む広い概念である。

#### 【0402】

また、前述の実施の形態には、次のような各種構成からなる発明が記載されている。

#### 【0403】

(1) 固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品（たとえば、腕時計、眼鏡、衣服等）に付されている無線識別子発信装置（RFIDタグ等）の固有の識別子（RFID等）を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップ（図15のSB1、SB3～SB7等）と、

前記個人ユーザに所持されるプライバシー保護用識別子発信装置（セキュリティ用のRFIDタグ1aまたはブラウザフォン30等）により、偽識別子（偽RFID等）を生成する偽識別子生成ステップ（図11のSA1～SA4、または、図26のSD2、SD10、SD12と図27のSE1～SE10と図29のSG3、SG3a、SG3b、SG5～SG9、図56、図57等）と、

識別子の送信要求があった場合に（図11のSA1または図29のSG3によりYESの判断があった場合に）、前記偽識別子生成ステップにより生成された前記偽識別子を前記プライバシー保護用識別子発信装置から発信する発信ステップ（図11のSA5、SA10、またはSG7、SG9等）と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取りステップ（図15のSB2、SB8、SB9～SB13）とを含み、

前記偽識別子生成ステップは、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成ステップ（図26のSD10、図27のSE1～SE10、図29のSG6～SG9、図56のRFID交換処理、図57のRFID交換処理等）を含むこと

を特徴とする、プライバシー保護方法。

【0404】

このような構成によれば、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにするために、購入済みの物品に付されている無線識別子発信装置の固有の識別子を利用したサービス等を個人ユーザが受けたいと思う必要な時に読取ってサービス等を享受することが可能となる。

【0405】

また、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取られる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

【0406】

(2) 固有の識別子(RFID等)が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置(セキュリティ用のRFIDタグ1aまたはブラウザフォン30等)を複数の個人ユーザに提供する提供ステップ(図13等)を含み、

前記プライバシー保護用識別子発信装置は、

偽識別子(偽RFID等)を生成する偽識別子生成手段(図11のSA1~SA4、または、図26のSD2、SD10、SD12と図27のSE1~SE10と図29のSG3、SG3a、SG3b、SG5~SG9、図56、図57等)と、

識別子の送信要求があった場合に(図11のSA1または図29のSG3によりYESの判断があった場合に)、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段(図11のSA5、SA10、または図29のSG7、SG9等)とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段(図26のSD10、図27のSE1~SE10、図29のSG6~SG9、図56のRFID交換処理、図57のRFID交換処理等)を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成して発信する前記プライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持する前記プライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子(図13の共通偽RFID等)を生成可能であり(図12と図13と図11のSA3、SA4、または図26のSD10、図27のSE1~SE10、図56のRFID交換処理、図57のRFID交換処理等)、

前記複数のプライバシー保護用識別子発信装置は、前記共通の偽識別子を他の偽識別子に比べて高い頻度で発信するプライバシー保護用識別子発信装置同士からなるグループであってグループ毎に前記共通の偽識別子が異なる複数のグループに分類され(図13の千代区、新宿区、渋谷区等の各地域を指定して販売される地域毎のグループに分類され)、

前記提供ステップは、前記それぞれのグループ毎に地域を指定して該グループに属する前記プライバシー保護用識別子発信装置を個人ユーザに提供する(図13の各地域を指定して個人ユーザに提供する)ことを特徴とする、プライバシー保護方法。

【0407】

このような構成によれば、プライバシー保護用識別子発信装置が複数の個人ユーザに提

供され、そのプライバシー保護用識別子発信装置は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成が可能であり、しかも、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報等を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

#### 【0408】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所でも読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという攪乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

#### 【0409】

さらに、複数のプライバシー保護用識別子発信装置は、前記共通の偽識別子を他の偽識別子に比べて高い頻度で発信するプライバシー保護用識別子発信装置同士からなるグループであってグループ毎に共通の偽識別子が異なる複数のグループに分類されており、それぞれのグループ毎に地域を指定してそのグループに属するプライバシー保護用識別子発信装置が個人ユーザに提供される。その結果、各地域内の者同士で共通の偽識別子を生成して発信する傾向が生じ、前述の異人物同一識別子発信現象を極力各地域内の個人ユーザ同士で生じさせることができ、悪意のプライバシー侵害者に対する前述した攪乱効果をより効果的に発揮することができる。

#### 【0410】

(3) 固有の識別子(RFID等)が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置(セキュリティ用のRFIDタグ1a、またはブラウザフォン30等)を複数の個人ユーザに提供する提供ステップ(図13等)を含み、

前記プライバシー保護用識別子発信装置は、

偽識別子を生成する偽識別子生成手段(図11のSA1~SA4、または、図26のSD2、SD10、SD12と図27のSE1~SE10と図29のSG3、SG3a、SG3b、SG5~SG9、図56、図57等)と、

識別子の送信要求があった場合に(図11のSA1または図29のSG1によりYESの判断があった場合に)、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段(図11のSA5、SA10、または図29のSG7、SG9等)とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段(図11のSA3、SA4、または図26のSD10、図27のSE1~SE10、図29のSG6~SG9、図56のRFID交換処理、図57のRFID交換処理等)を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライ

バシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子（図12のRが0～39に属する列のRFIDのコードデータ、図13の共通偽RFID、または図27、図56、図57により互いに交換された偽RFID等）を生成可能であり、

前記提供ステップにより或る個人ユーザに提供されたプライバシー保護用識別子発信装置（図12（a）のテーブルを記憶しているRFIDタグ1a等）から、予め定められた所定個数（たとえば1個）の偽識別子を1度に発信し（図11のSA4、SA5と図12（a）のRFID等）、

前記提供ステップにより前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置（図12（b）（c）のテーブルを記憶しているRFIDタグ1a等）から、前記所定個数（たとえば1個）よりも多い複数（たとえば4個）の偽識別子（図12（b）（c）のRFID1～4）を1度に発信し、該複数の偽識別子のうちの前記所定個数を除く他の偽識別子（図12（a）（c）のRFID2～4）を前記共通の偽識別子として生成することを特徴とする、プライバシー保護方法。

#### 【0411】

このような構成によれば、プライバシー保護用識別子発信装置が複数の個人ユーザに提供され、そのプライバシー保護用識別子発信装置は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成が可能であり、しかも、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報等を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

#### 【0412】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所でも読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという攪乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

#### 【0413】

また、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が一度に発信される一方、前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から前述の所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信される。その結果、個人ユーザに携帯された購入済物品に付されている無線識別子発信装置が常時識別子が発信される状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0414】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、1度に

複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。その結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

#### 【0415】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前述の所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と携帯している購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザから発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数（所定個数）を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

#### 【0416】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物間で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができ、プライバシーを極力保護することができる。

#### 【0417】

(4) 固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置（セキュリティ用のRFIDタグ1aまたはブラウザフォン30等）であって、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図11のSA1～SA4、または、図26のSD2、SD10、SD12と図27のSE1～SE10と図29のSG3、SG3a、SG3b、SG5～SG9、図56、図57等）と、

識別子の送信要求があった場合に（図11のSA1または図29のSG3によりYESの判断があった場合に）、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段（図11のSA5、SA10、またはSG7、SG9等）を含むことを特徴とする、プライバシー保護用識別子発信装置。

#### 【0418】

このような構成によれば、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取ら

れる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

【0419】

(5) 前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置(RFIDタグ等)の各々が発信する識別子の範囲内で前記偽識別子を生成することを特徴とする、(4)に記載のプライバシー保護用識別子発信装置

。

【0420】

このような構成によれば、既に販売済みとなっている商品それぞれに付された無線識別子発信装置の各々が発信する識別子の範囲内で可変型の偽識別子が生成されて発信されるために、発信された偽識別子が既に消費者の購入済み商品に付された無線識別子発信装置から発信される識別子と区別することができず、発信された識別子が偽の識別子であると見破られてしまう不都合を極力防止することができる。

【0421】

(6) 前記発信手段は、前回の偽識別子の発信から所定時間内(たとえば5秒内)に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信する(図11のSA2、SA10、または図29のSG3a、SG3b等)ことを特徴とする、(4)または(5)に記載のプライバシー保護用識別子発信装置。

【0422】

このような構成によれば、発信手段が、前回の識別子の発信から所定時間内に再度識別子の送信要求があった場合に前回発信した識別子と同じ識別子を発信するために、識別子読取装置側における読取り制度の信頼性の向上等のために複数回連続して識別子の発信要求を送信して連続して複数回識別子を読取る方式が採用されたとしても、同じ偽識別子が発信されるために、連続して複数回読取られた識別子が異なることによる不都合を極力防止することができる。また、可変型の偽識別子であるかまたは本物の無線識別子発信装置から発信された固有の識別子であるかをチェックすることを目的として、前述と同様に複数回連続して識別し発信要求を送信して連続的に識別子を読取ることが行われたとしても、可変型の偽識別子であることが見破られてしまう不都合を極力防止することができる。

【0423】

(7) 前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能(図12のRが0~39の領域に属する列のRFIDを生成可能、または図27や図56や図57のRFID交換処理で互いに交換した偽RFIDを生成可能)であることを特徴とする、(4)~(6)のいずれかに記載のプライバシー保護用識別子発信装置。

【0424】

このような構成によれば、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象(異人物同一識別子発信現象)を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報等を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【0425】



しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという攪乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

#### 【0426】

(8) 他のプライバシー保護用識別子発信装置（ブラウザフォン30等）と交信する交信手段（図27、図56、図57のRFID交換処理）をさらに含み、

前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段（図27、図56、図57のSE9、SE10とEEPROM194等）を含み、

前記交信手段は、前記他のプライバシー保護用識別子発信装置と交信して（図27の直接電波交信、図56の通話交信、図57の電子メール交信等）、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信するとともに（図27のSE6、SE8、または図56のSS8、SE9、SE10、または図57のSE6、ST3等）当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて（図27のSE7～SE10、または図56のSE7、SS8、または図57のST8、SE9、SE10等）、記憶している互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に（図29のSG3によりYESの判断があった場合に）、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成する（図29のSG9等）ことを特徴とする、(7)に記載のプライバシー保護用識別子発信装置。

#### 【0427】

このような構成によれば、プライバシー保護用識別子発信装置同士で交信して、互いに記憶している識別子同士を送受信して互いの識別子を交換する。そして、識別子の送信要求があった場合には、前述した交換後の識別子が前述の共通の偽識別子として生成されて発信される。その結果、互いに交信して識別子を交換するという比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0428】

なお、1度に発信される複数の識別子同士を交換し、識別子の送信要求があった場合に、該複数の識別子を1度に全て発信してもよいが、該複数の識別子の内の所定個数を他の偽識別子（たとえば乱数を利用して生成されたランダムな偽識別子）に変換する変換手段を設け、変換した後の状態の複数の識別子を発信するようにし、前述の異人物間での複数識別子中所定個数可変型現象が生じるようにしてもよい。

#### 【0429】

(9) 前記交信手段は、互いの識別子を交換するときの交信可能通信限界距離が20メートル以内に定められており、該交信可能通信限界距離圏内に進入した他のプライバシー保護用識別子発信装置と交信して互いの識別子を交換する（図27のSE1、SE2等）ことを特徴とする、(8)に記載のプライバシー保護用固有識別子発信装置。

#### 【0430】

このような構成によれば、互いの識別子を交換するときの交信可能通信限界距離が20メートル以内に定められており、その交信可能通信限界距離圏内に進入したプライバシー保護用識別子発信装置と互いに交信して識別子が交換されるために、20メートル以内という比較的近距离圏内に位置する個人ユーザの間で互いの識別子の交換がなされることとなり、比較的近くに位置していた者同士で共通の偽識別子を共有して発信できる状態となり、前述の異人物同一識別子発信現象を極力近距离圏内に位置していた個人ユーザ同士で



生じさせることができ、悪意のプライバシー侵害者に対する前述した攪乱効果をより効果的に発揮することができる。

#### 【0431】

(10) 前記交信手段は、既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内（たとえば1日以内）に再度前記識別子の交換を行なうことを禁止する禁止手段（図27図、図56、図57のSE3等）を有することを特徴とする、(8)または(9)に記載のプライバシー保護用識別子発信装置。

#### 【0432】

このような構成によれば、既に交信して識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度識別子の交換を行なうことを防止でき、既に識別子交換済みの相手と所定期間内に再度識別子の交換を行なうという無駄を防止することができる。

#### 【0433】

(11) 前記交信手段は、電話機能（ブラウザフォン30による通話機能）を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し（図56のRFID交換処理等）、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成する（図29のSG9）ことを特徴とする、(8)～(10)のいずれかに記載のプライバシー保護用識別子発信装置。

#### 【0434】

このような構成によれば、交信手段が電話機能を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0435】

(12) 前記交信手段は、電子メール機能（ブラウザフォン30によるEメール機能等）を有しており、電子メールの送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し（図57のSE5、SE6、ST3等）、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ（図57のST8、SE9、SE10等）、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読み出すことにより前記共通の偽識別子として生成する（図29のSG9）ことを特徴とする、(8)～(11)のいずれかに記載のプライバシー保護用識別子発信装置。

#### 【0436】

このような構成によれば、交信手段が電子メール機能を有しており、電子メールの送信とともに識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して識別子記憶手段に記憶させることにより互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0437】

(13) 前記発信手段は、他のプライバシー保護用識別子発信装置（図12(a)のテーブルを記憶しているRFIDタグ1a等）から1度に発信される所定個数（たとえば1個）の偽識別子よりも多い複数の偽識別子を1度に発信可能であり（図12(b)(c)の4個のRFID1～4、図11のAS4、AS5等）、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数（たとえば1個）を除く他の偽識別子を前記共通の偽識別子として生成する（図12(a)(c)の

RFID 2~4 を共通の偽 RFID として生成する) ことを特徴とする、(4) ~ (12) のいずれかに記載のプライバシー保護用識別子発信装置。

#### 【0438】

このような構成によれば、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が1度に発信される一方、前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から前記所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前記共通の偽識別子として生成されて発信される。その結果、個人ユーザに所持された購入済物品から他人が固有の識別子を読取ることのできる状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0439】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、1度に複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所での識別子が発信された時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象(複数識別子中所定個数可変型現象)が生ずる。その結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

#### 【0440】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前記所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザが発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数(所定個数)を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複数箇所での識別子が発信された時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは所持品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象(複数識別子中所定個数可変型現象)が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

。

#### 【0441】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができ、プライバシーを極力保護することができる。

#### 【0442】

(14) 購入されることにより個人ユーザの所持品となった物品(たとえば、腕時計、眼鏡、衣服等)に付されている無線識別子発信装置(RFIDタグ等)の固有の識別子

(RFID等)を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段(図15のSB1、SB3~SB7等)と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段(図15のSB2、SB8、SB9~SB13)とを、さらに含むことを特徴とする、(4)~(13)のいずれかに記載のプライバシー保護用識別子発信装置。

#### 【0443】

このような構成によれば、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を個人ユーザの意思に従って読取ることができるようにするために、購入済みの物品に付されている無線識別子発信装置の固有の識別子を利用したサービス等を個人ユーザが受けたいと思う必要なときに読取ってサービス等を享受することが可能となる。

#### 【0444】

(15) 前記識別子ガード手段は、本人認証のための固有識別情報(たとえばパスワード)を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え(図15のSB3~SB8等)、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にする(図15のSB8、SB9~SB13等)ことを特徴とする、(14)に記載のプライバシー保護用識別子発信装置。

#### 【0445】

このような構成によれば、識別子ガード手段により、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、読取り手段により、固有識別情報を発信して無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にするために、確実に無線識別子発信装置の識別子をガードした状態にできるとともに、本人認証が行われた本人のみが無線識別子発信装置を識別子発信可能状態にすることができ、セキュリティを向上させることができる。

#### 【0446】

(16) 固有の識別子(RFID等)が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

個人ユーザのプライバシーを保護するために匿名(トラップ型バーチャルパーソンE(B13P)等)を名乗り匿名ユーザ(トラップ型バーチャルパーソン)として行動するために作成された匿名(E(B13P)等)と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関(金融機関7等)において登録する処理を行なう登録処理ステップ(図17のS15、図19のS440等)と、

前記匿名ユーザ用の電子証明書を発行する電子証明書発行ステップ(図17のS17、図19のS441等)と、

前記匿名ユーザの住所を、該匿名に対応する個人ユーザとは異なった住所に設定するための住所設定ステップ(図17のS9~S12等)と、

所定の業者(たとえば、百貨店等の商品販売業者等)にユーザ登録するときに(たとえばポイントカードの新規発行時の顧客登録のときに)前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録ステップ(図32(b)のSJ1~SJ8と図33のSK2、SK21~SK24、SK18~SK20等)と、

識別子の送信要求があった場合に(図29のSG3によりYESの判断があった場合に)、前記個人ユーザに所持されるプライバシー保護用識別子発信装置(ブラウザフォン30等)から偽識別子を発信する発信ステップ(図29のSG3~SG13等)と、

前記ユーザ登録ステップにより前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図32のSJ8、図9、EEPROM26等）とを含み、

前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図29のSG4、SG10～SG12等）ことを特徴とする、プライバシー保護方法。

#### 【0447】

このような構成によれば、個人ユーザのプライバシーを保護するために匿名を作成しその匿名を名乗って行動する匿名ユーザ用の電子証明書が発行されるため、匿名ユーザでありながらも発行された電子証明書を提示することにより売買等の取引行為の主体になることが可能となる。しかも、匿名ユーザの住所が、該匿名に対応する個人ユーザとは異なった住所に設定されているために、住所を手がかりにどの個人ユーザがどの匿名ユーザに該当するのを見破られてしまう不都合も極力防止できる。また、所定の業者にユーザ登録するときに匿名の情報を登録して匿名ユーザとして登録するため、該業社に対して匿名を名乗り匿名ユーザとして行動することができ、個人ユーザ本人のプライバシーを守りながらも該業社に対し売買等の取引行為を行なうことができるとともに、ユーザ登録によるサービス等を楽しむことができる。

#### 【0448】

一方、匿名を登録した業社に対して匿名ユーザとして行動しているときに該匿名ユーザから発信された識別子がその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより業社側は、たとえば、移動する匿名ユーザから発せられる識別情報を要所所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、匿名を登録した業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、匿名を登録している業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

#### 【0449】

(17) 前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合でないときであっても（図29のSG10によりNOの判断がなされるときであっても）、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には（図28のSF7aによりYESの判断がなされSF7bにより業者の選択指定が記憶された場合には）、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図29のSG13等）ことを特徴とする、(16)に記載のプライバシー保護方法。

#### 【0450】

このような構成によれば、匿名を登録している業者に対し偽識別子を発信する場合でないときであっても、匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信することができる。その結果、その匿名用識別子を受信した業社から該匿名用識別子に対応する匿名宛にダイレクトメールや電子メールが送られてきた場合には、その匿名をユーザ登録している業社からメールを送ってきた業社に匿名情報が横流しされたことが判明でき、個人情報の横流しを監視することが可能となる。

#### 【0451】

(18) 固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護システムであって、

個人ユーザのプライバシーを保護するために匿名（トラップ型バーチャルパーソン E（B13P）等）を名乗り匿名ユーザ（トラップ型バーチャルパーソン）として行動するために作成された匿名（E（B13P）等）と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関（金融機関 7 等）において登録する処理を行なう登録処理手段（図 17 の S15、図 19 の S440 等）と、

所定の業者（たとえば、百貨店等の商品販売業者等）にユーザ登録するときに（たとえばポイントカードの新規発行時の顧客登録のときに）前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録手段（図 32（b）の SJ1～SJ8 と図 33 の SK2、SK21～SK24、SK18～SK20 等）と、

識別子の送信要求があった場合に（図 29 の SG3 により YES の判断があった場合に）、前記個人ユーザに所持されるプライバシー保護用識別子発信装置（ブラウザフォン 30 等）から偽識別子を発信する発信手段（図 29 の SG3～SG13 等）と、

前記ユーザ登録手段により前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図 32 の SJ8、図 9、EEPROM26 等）とを含み、

前記発信手段は、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図 29 の SG4、SG10～SG12 等）ことを特徴とする、プライバシー保護システム。

#### 【0452】

このような構成によれば、所定の業者にユーザ登録するときに匿名の情報を登録して匿名ユーザとして登録するため、該業社に対して匿名を名乗り匿名ユーザとして行動することができ、個人ユーザ本人のプライバシーを守りながらもユーザ登録によるサービス等を享受することができる。

#### 【0453】

一方、匿名を登録した業社に対して匿名ユーザとして行動しているときに該匿名ユーザから発信された識別子がその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより、たとえば、業社側は移動する匿名ユーザから発せられる識別情報を要所要所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、匿名を登録した業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、匿名を登録している業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

#### 【0454】

(19) 固有の識別子（RFID）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置（ブラウザフォン 30 等）であって、

所定の業者（たとえば、百貨店等の商品販売業者等）に対し個人ユーザが匿名（トラップ型バーチャルパーソン E（B13P）等）を名乗り匿名ユーザ（トラップ型バーチャルパーソン）として行動する場合に前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図 32 の SJ8、図 9、EEPROM26 等）と

識別子の送信要求があった場合に（図 29 の SG3 により YES の判断があった場合に）偽識別子を発信する手段であって、前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する発信手段（図 29 の SG4、SG10～SG12 等）とを含むことを特徴とする、プ

バシー保護用識別子発信装置。

【0455】

このような構成によれば、所定の業者に対し個人ユーザが匿名を名乗り匿名ユーザとして行動する場合に前記業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、識別子の送信要求があった場合に、前記業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信する。業社に対して匿名ユーザとして行動しているときに該匿名ユーザから発信された識別子がその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより、たとえば、業社側は移動する匿名ユーザから発せられる識別情報を要所所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、前記業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、前記業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

【0456】

(20) 前記発信手段は、個人ユーザが匿名を名乗る前記業者に対し前記偽識別子を発信する場合でないときであっても(図29のSG10によりNOの判断がなされるときであっても)、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には(図28のSF7aによりYESの判断がなされSF7bにより業者の選択指定が記憶された場合には)、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する(図29のSG13等)ことを特徴とする、(19)に記載のプライバシー保護用識別子発信装置。

【0457】

このような構成によれば、個人ユーザが匿名を名乗る前記業者に対し前記偽識別子を発信する場合でないときであっても、匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信することができる。その結果、その匿名用識別子を受信した業社から該匿名用識別子に対応する匿名宛にダイレクトメールや電子メールが送られてきた場合には、個人ユーザが匿名を名乗る前記業者からメールを送ってきた業社に匿名情報が横流しされたことが判明でき、個人情報の横流しを監視することが可能となる。

【0458】

(21) 前記所定の業者は、商品を販売する販売店(図30の百貨店206等)であり、

前記匿名用偽識別子記憶手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に匿名ユーザとして登録した当該販売店に対応する匿名用偽識別子を記憶しており(図32のSJ8、図9参照)、

前記発信手段は、前記販売店において購入した商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の価格を支払うための自動決済を行う際に(図31の自動決済処理を行う際に)、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に(図29のSG10によりYESの判断がなされた場合に)、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する(図29のSG4、SG10~SG12等)ことを特徴とする、(19)または(20)に記載のプライバシー保護用識別子発信装置。

【0459】

このような構成によれば、販売店においてポイントカードの発行に伴うユーザ登録の際



に匿名ユーザとして登録することにより、当該販売店において匿名ユーザとして行動して商品購入等を行なうことができ、個人ユーザのプライバシーを保護しながらもポイント付与のサービスも享受できる。また、販売店において購入した商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の価格を支払うための自動決済を行う際に、無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、匿名用偽識別子が匿名用偽識別子記憶手段から読出されて発信されるために、自動決済を行なうことができながらも、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

**【0460】**

(22) 前記匿名用偽識別子記憶手段は、複数の前記業者（たとえば、ABC、MTT、MEC等）に対応してそれぞれ異なった匿名用偽識別子（たとえば、abc、mtt、mec等）を記憶しており（図9参照）、

前記発信手段は、前記複数の業者のうちのいずれに個人ユーザが匿名を名乗るかに応じて、当該匿名を名乗る業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から選択して発信する（図29のSG11、SG12等）ことを特徴とする、(19)～(21)のいずれかに記載のプライバシー保護用識別子発信装置。

**【0461】**

このような構成によれば、匿名用偽識別子記憶手段は、複数の前記業者に対応してそれぞれ異なった匿名用偽識別子を記憶しており、発信手段は、複数の業者のうちのいずれに個人ユーザが匿名を名乗るかに応じて、当該匿名を名乗る業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から選択して発信するために、業社毎に異なった匿名用識別子を使分けることができる。

**【0462】**

(23) 固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプログラムであって、

プライバシー保護用識別子発信装置セキュリティ用のRFIDタグ1aまたはブラウザフォン30等）に設けられているコンピュータ（ロジック100、ROM101、RAM102、EEPROM103、またはLSIチップ20等）に、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図11のSA1～SA4、または、図26のSD2、SD10、SD12と図27のSE1～SE10と図29のSG3、SG3a、SG3b、SG5～SG9、図56、図57等）と、

識別子の送信要求があった場合に（図11のSA1または図29のSG3によりYESの判断があった場合に）、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段（図11のSA5、SA10、またはSG7、SG9等）と、

して機能させるための、プログラム。

**【0463】**

このような構成によれば、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取られる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

**【0464】**

(24) 前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置（RFIDタグ等）の各々が発信する識別子の範囲内で前記偽識別子を生成させることを特徴とする、(23)に記載のプログラム。

**【0465】**

このような構成によれば、既に販売済みとなっている商品それぞれに付された無線識別



子発信装置の各々が発信する識別子の範囲内で可変型の偽識別子が生成されて発信されるために、発信された偽識別子が既に消費者の購入済み商品に付された無線識別子発信装置から発信される識別子と区別することができず、発信された識別子が偽の識別子であると見破られてしまう不都合を極力防止することができる。

**【0466】**

(25) 前記発信手段は、前回の偽識別子の発信から所定時間内（たとえば5秒内）に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信させる（図11のSA2、SA10、または図29のSG3a、SG3b等）ことを特徴とする、(23) または(24)に記載のプログラム。

**【0467】**

このような構成によれば、発信手段が、前回の識別子の発信から所定時間内に再度識別子の送信要求があった場合に前回発信した識別子と同じ識別子を発信するために、識別子読取装置側における読取り制度の信頼性の向上等のために複数回連続して識別子の発信要求を送信して連続して複数回識別子を読取る方式が採用されたとしても、同じ偽識別子が発信されるために、連続して複数回読取られた識別子が異なることによる不都合を極力防止することができる。また、可変型の偽識別子であるかまたは本物の無線識別子発信装置から発信された固有の識別子であるかをチェックすることを目的として、前述と同様に複数回連続して識別し発信要求を送信して連続的に識別子を読取ることが行われたとしても、可変型の偽識別子であることが見破られてしまう不都合を極力防止することができる。

**【0468】**

(26) 前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能（図12のRが0～39の領域に属する列のRFIDを生成可能、または図27や図56や図57のRFID交換処理で互いに交換した偽RFIDを生成可能）にすることを特徴とする、(23)～(25)のいずれかに記載のプログラム。

**【0469】**

このような構成によれば、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報に不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

**【0470】**

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所を読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという攪乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

**【0471】**

(27) 前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段（図27

、図56、図57のSE9、SE10とEEPROM194等)を含み、

前記他のプライバシー保護用識別子発信装置と交信して(図27の直接電波交信、図56の通話交信、図57の電子メール交信等)、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信させるとともに(図27のSE6、SE8、または図56のSS8、SE9、SE10、または図57のSE6、ST3等)当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて(図27のSE7~SE10、または図56のSE7、SS8、または図57のST8、SE9、SE10等)、記憶している互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に(図29のSG3によりYESの判断があった場合に)、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成させる(図29のSG9等)ことを特徴とする、(26)に記載のプログラム。

#### 【0472】

このような構成によれば、プライバシー保護用識別子発信装置同士で交信して、互いに記憶している識別子同士を送受信して互いの識別子を交換する。そして、識別子の送信要求があった場合には、前述した交換後の識別子が前述の共通の偽識別子として生成されて発信される。その結果、互いに交信して識別子を交換するという比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0473】

(28) 既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内(たとえば1日以内)に再度前記識別子の交換を行なうことを禁止する禁止手段(図27図、図56、図57のSE3等)として機能させることを特徴とする、(26)または(27)に記載のプログラム。

#### 【0474】

このような構成によれば、既に交信して識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度識別子の交換を行なうことを防止でき、既に識別子交換済みの相手と所定期間内に再度識別子の交換を行なうという無駄を防止することができる。

#### 【0475】

(29) 電話(ブラウザフォン30による通話)で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し(図56のRFID交換処理等)、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成させる(図29のSG9)ことを特徴とする、(26)~(28)のいずれかに記載のプログラム。

#### 【0476】

このような構成によれば、交信手段が電話機能を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0477】

(30) 電子メール(ブラウザフォン30によるEメール)の送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し(図57のSE5、SE6、ST3等)、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ(図57のST8、SE9、SE10等)、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読

出すことにより前記共通の偽識別子として生成させる（図29のSG9）ことを特徴とする、（26）～（29）のいずれかに記載のプライバシー保護用識別子発信装置。

#### 【0478】

このような構成によれば、発信手段が電子メール機能を有しており、電子メールの送信とともに識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して識別子記憶手段に記憶させることにより互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0479】

（31） 前記発信手段は、他のプライバシー保護用識別子発信装置（図12（a）のテーブルを記憶しているRFIDタグ1a等）から1度に発信される所定個数たとえば1個）の偽識別子よりも多い複数の偽識別子を1度に発信させることが可能であり図12（b）（c）の4個のRFID1～4、図11のAS4、AS5等）、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成させる（図12（a）（c）のRFID2～4を共通の偽RFIDとして生成する）ことを特徴とする、（23）～（30）のいずれかに記載のプログラム。

#### 【0480】

このような構成によれば、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が1度に発信される一方、前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から前記所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前記共通の偽識別子として生成されて発信される。その結果、個人ユーザに所持された購入済物品から他人が固有の識別子を読取ることのできる状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

#### 【0481】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、1度に複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。その結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

#### 【0482】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前記所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザが発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数（所定個数）を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複数箇所で識別子が

読取られた時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは所持品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

#### 【0483】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができる。

#### 【0484】

(32) 購入されることにより個人ユーザの所持品となった物品（たとえば、腕時計、眼鏡、衣服等）に付されている無線識別子発信装置（RFIDタグ等）の固有の識別子（RFID等）を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段（図15のSB1、SB3～SB7等）と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段（図15のSB2、SB8、SB9～SB13）と、

して機能させるプログラムをさらに含むことを特徴とする、(23)～(31)のいずれかに記載のプログラム。

#### 【0485】

このような構成によれば、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を個人ユーザの意思に従って読取ることができるようにするために、購入済みの物品に付されている無線識別子発信装置の固有の識別子を利用したサービスを個人ユーザが受けたいと思う必要なときに読取ってサービスを享受することが可能となる。

#### 【0486】

(33) 前記識別子ガード手段は、本人認証のための固有識別情報（たとえばパスワード）を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え（図15のSB3～SB8等）、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にさせる（図15のSB8、SB9～SB13等）ことを特徴とする、(32)に記載のプログラム。

#### 【0487】

このような構成によれば、識別子ガード手段により、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、読取り手段により、固有識別情報を発信して無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にするために、確実に無線識別子発信装置の識別子をガードした状態にできるとともに、本人認証が行われた本人のみが無線識別子発信装置を識別子発信可能状態にすることができ、セキュリティを向上させることができる。

#### 【0488】

[構成と実施形態との対応関係]

次に、本発明の構成と実施の形態との対応関係を、本発明の構成中に実施の形態の開示内容を括弧書き挿入して示す。

【0489】

(1) 個人ユーザに関する固有の識別子（たとえば、RFID）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品（たとえば、眼鏡、衣服、腕時計等）に付されている無線識別子発信装置（たとえば、RFIDタグ）の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップ（たとえば、図15のSB1～SB8）と、

前記個人ユーザが顧客またはユーザとして所定の業者（たとえば、MTT、百貨店206等）に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレス（たとえば、図61の#e9¥82%31&0α3t\*c）を生成して当該業社に通知するための処理を行うメールアドレス通知処理ステップ（たとえば、図59のSU1～SU7、S1000～S1003）と、

前記メールアドレス通知処理ステップにより前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成ステップ（たとえば、図35のS273～S279）と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成ステップにより生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信ステップ（たとえば、図28のSF7a、SF7b、図29のSG4、SG10～SG13）と、

送信元から送信された電子メールを指定されたメールアドレスに従って送信先に送信するための電子メール送信ステップ（たとえば、図20のS514～S521または図60のSV2、SV5～SV16）と、

該電子メール送信ステップにより送信される電子メールの送信先のメールアドレスが、前記メールアドレス通知処理ステップにより通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否かを監視する監視ステップ（たとえば、図60のSV5～SV12）を含むことを特徴とする、プライバシー保護方法。

【0490】

(2) 個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護システムであって、

前記個人ユーザが顧客またはユーザとして所定の業者（たとえば、MTT、百貨店206等）に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレス（たとえば、図61の#e9¥82%31&0α3t\*c）を生成して当該業社に通知するための処理を行うメールアドレス通知処理手段（たとえば、図59のSU1～SU7、S1000～S1003）と、

前記メールアドレス通知処理手段により前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段（たとえば、図35のS273～S279）と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信

手段（たとえば、図28のSF7a、SF7b、図29のSG4、SG10～SG13）と、

送信元から送信された電子メールの送信先のメールアドレスが、前記メールアドレス通知処理手段により通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否かを監視する監視手段（たとえば、図60のSV5～SV12）とを含むことを特徴とする、プライバシー保護システム。

【0491】

(3) 前記メールアドレス通知処理手段は、メールアドレスを通知する通知業社を特定するための通知業社特定情報を含むデータを暗号化して前記通知用メールアドレスを生成する暗号化生成手段（たとえば、図59のS1001、S1002）を含み、

前記監視手段は、

送信元から送信された電子メールの通知用メールアドレスを復号する復号手段（たとえば、図60のSV5～SV7）と、

該復号手段により復号されたデータ中に含まれている前記通知業社特定情報と当該電子メールの送信元の情報とが一致するか否かを判定する判定手段（たとえば、図60のSV8～SV12）とを含むことを特徴する、請求項2に記載のプライバシー保護システム。

【0492】

(4) 前記通知業者は、商品を販売する販売店（たとえば、百貨店206）であり、前記メールアドレス通知処理手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に当該販売店に対応する通知用メールアドレスを生成して通知する処理を行い（たとえば、図32のSJ1～SJ9）、

前記発信手段は、前記販売店において購入する商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の販売価格に従って自動決済を行う際に（たとえば、）、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に（たとえば、図31の自動決済処理による自動決済時に）、前記販売店に対応する前記通知業者用識別子を発信する（たとえば、図31のSH2により受信した販売業者の店名信号に応じて図29のSG10→SG11→SG12と進み、受信した業社に対応するトラップ型RFIDを発信する）ことを特徴とする、請求項2または請求項3に記載のプライバシー保護システム。

【0493】

(5) 個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置であって、

前記個人ユーザが顧客またはユーザとなった所定の業者のために新たな通知用メールアドレスを生成して当該業社に通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段（たとえば、図35のS273～S279）と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段（たとえば、図28のSF7a、SF7b、図29のSG4、SG10～SG13）とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【0494】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【0495】



【図1】 プライバシー保護システムの全体構成を示す概略システム図である。

【図2】 金融機関に設置されたデータベースに記憶されている各種データを示す説明図である。

【図3】 金融機関に設置されたデータベースに記憶されている各種データを示す説明図である。

【図4】 金融機関に設置されているデータベースに記憶されている各種データを示す説明図である。

【図5】 XMLストアのデータベースに記憶されている各種データを示す説明図である。

【図6】 コンビニエンスストアに設置されているデータベースに記憶されている各種情報を説明するための説明図である。

【図7】 ユーザ端末の一例としてのブラウザフォンを示す正面図である。

【図8】 ユーザ端末の一例としてのブラウザフォンを示す正面図である。

【図9】 VP用IC端末のトラップ型RFID記憶領域に記憶されているトラップ型RFIDデータの内訳を示す図である。

【図10】 セキュリティ用のRFIDタグおよびその回路ブロック図

【図11】 セキュリティ用のRFIDタグの制御プログラムを示すフローチャート

【図12】 セキュリティ用のRFIDタグに記憶されているテーブル

【図13】 セキュリティ用のRFIDタグの地域を指定しての販売の方法を説明する説明図

【図14】 ブラウザフォンの制御プログラムを示すフローチャート

【図15】 RFIDタグ切換え処理のサブルーチンプログラムを示すフローチャート

【図16】 購入商品に付されているRFIDタグの制御プログラムを示すフローチャート

【図17】 VP管理サーバの処理動作を示すフローチャート

【図18】 (a)はVP管理サーバの処理動作を示すフローチャートであり、(b)は個人情報の登録処理のサブルーチンプログラムを示すフローチャート

【図19】 トラップ情報の登録処理のサブルーチンプログラムを示すフローチャート

【図20】 メール転送、流通チェックのサブルーチンプログラムを示すフローチャート

【図21】 認証用サーバの処理動作を示すフローチャート

【図22】 決済サーバの処理動作を示すフローチャート

【図23】 決済サーバの処理動作を示すフローチャート

【図24】 (a)は決済処理のサブルーチンの一部、(b)は正当機関証明処理のサブルーチンプログラムを示すフローチャート

【図25】 クレジットカード発行会社からの問合せ処理のサブルーチンプログラムを示すフローチャート

【図26】 ブラウザフォンの偽モード処理のサブルーチンプログラムを示すフローチャート

【図27】 ブラウザフォンのRFID交換処理のサブルーチンプログラムを示すフローチャート

【図28】 ブラウザフォンのトラップモード処理のサブルーチンプログラムを示すフローチャート

【図29】 ブラウザフォンのRFID発信処理のサブルーチンプログラムを示すフローチャート

【図30】 RFIDタグを利用した百貨店での自動決済の説明図

【図31】 ブラウザフォンの自動決済処理のサブルーチンプログラムを示すフローチャート

【図32】 (a)はブラウザフォンのポイントカード加算処理のサブルーチンプログラムを示すフローチャート、(b)はブラウザフォンのポイントカード登録処理のサ



ブルーチンプログラムを示すフローチャート

【図33】 販売業者決済サーバの制御用プログラムを示すフローチャート

【図34】 VP用IC端末の処理動作を示すフローチャート

【図35】 (a) は暗証番号チェック処理のサブルーチンプログラムを示すフローチャートであり、(b) はトラップ型RFID処理のサブルーチンプログラムを示すフローチャートであり、(c) は本人証明処理(VP用)のサブルーチンプログラムを示すフローチャートである。

【図36】 (a) はデータ入力処理のサブルーチンプログラムを示すフローチャートであり、(b) はユーザエージェント動作処理のサブルーチンプログラムを示すフローチャートであり、(c) はリロード金額の使用処理のサブルーチンプログラムを示すフローチャートであり、(d) はVP署名処理のサブルーチンプログラムを示すフローチャートである。

【図37】 トラップ型VP処理のサブルーチンプログラムを示すフローチャートである。

【図38】 コンビニサーバの処理動作を示すフローチャートである。

【図39】 コンビニサーバの処理動作を示すフローチャートであり、(a) は暗証番号チェック処理のサブルーチンプログラムを示すフローチャートであり、(b) は本人チェック処理のサブルーチンプログラムを示すフローチャートであり、(c) は決済処理のサブルーチンプログラムを示すフローチャートである。

【図40】 (a) は、VP用IC端末に記憶されているトラップ情報であり、(b) は、トラップ型VP処理のサブルーチンプログラムを示すフローチャートであり、(c) は、VP用IC端末の制御動作を示すフローチャートである。

【図41】 商品情報提供サービスシステムの全体概略を示す構成図である。

【図42】 商品情報サービス業者のWebデータベースに記憶されている商品ホームページを示す説明図である。

【図43】 商品情報サービス業者のWebサーバの制御用プログラムを示すフローチャートの一部である。

【図44】 商品情報サービス業者のWebサーバの制御用プログラムを示すフローチャートの一部である。

【図45】 ブラウザフォンの商品検索・購入処理のサブルーチンプログラムを示すフローチャートの一部である。

【図46】 ブラウザフォンの商品検索・購入処理のサブルーチンプログラムを示すフローチャートの一部である。

【図47】 生産者のWebサーバの制御用プログラムを示すフローチャートである。

【図48】 住所、氏名、Eメールアドレスの送信処理のサブルーチンプログラムを示すフローチャートである。

【図49】 VP出生依頼処理のサブルーチンプログラムを示すフローチャートである。

【図50】 (a) は正当機関チェック処理のサブルーチンプログラムを示すフローチャートであり、(b) は電子証明書発行要求処理のサブルーチンプログラムを示すフローチャートである。

【図51】 (a) はVP用入力処理のサブルーチンプログラムを示すフローチャートであり、(b) はRP用入力処理のサブルーチンプログラムを示すフローチャートである。

【図52】 SETによる決済処理の概要を説明するための説明図である。

【図53】 VP用決済処理のサブルーチンプログラムを示すフローチャートである。

【図54】 (a) は本人証明処理のサブルーチンプログラムを示すフローチャートであり、(b) はVP用決済処理のサブルーチンプログラムの一部を示すフローチャートである。

【図55】 VP用決済処理のサブルーチンプログラムの一部を示すフローチャートで

ある。

【図 56】別実施の形態におけるブラウザフォンの R F I D 交換処理のサブルーチンプログラムを示すフローチャートである。

【図 57】別実施の形態におけるブラウザフォンの R F I D 交換処理のサブルーチンプログラムを示すフローチャートである。

【図 58】メールサーバのデータベースに記憶されているデータを説明するための説明図である。

【図 59】(a) は、ブラウザフォンによる E メールアドレス通知処理のサブルーチンプログラムを示すフローチャートである、(b) は、I C 端末による E メールアドレス生成処理のサブルーチンプログラムを示すフローチャートである。

【図 60】メールサーバの制御処理を示すフローチャートである。

【図 61】図 59、図 60 に示した制御内容を分かり易く説明するための説明図である。

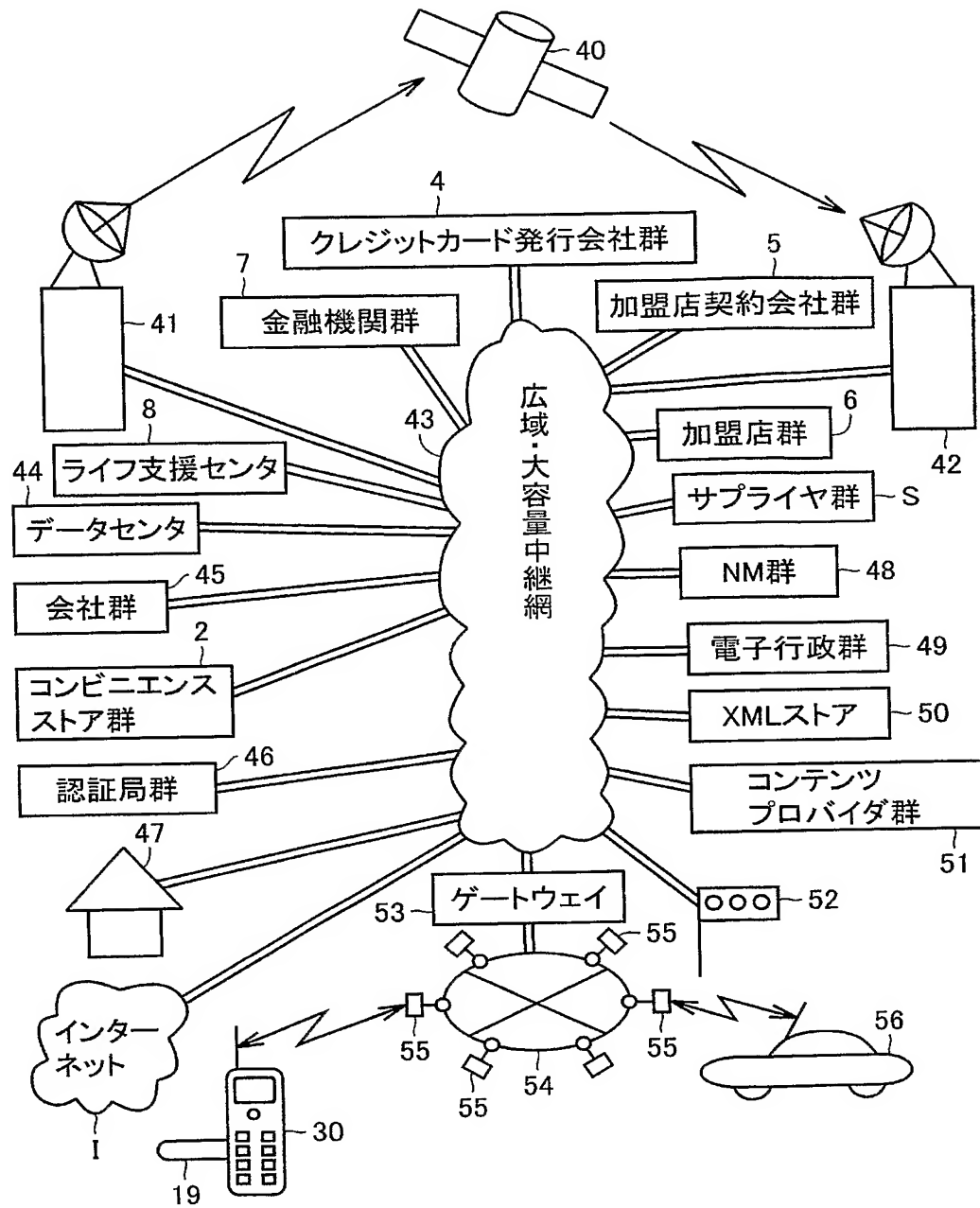
【符号の説明】

【0496】

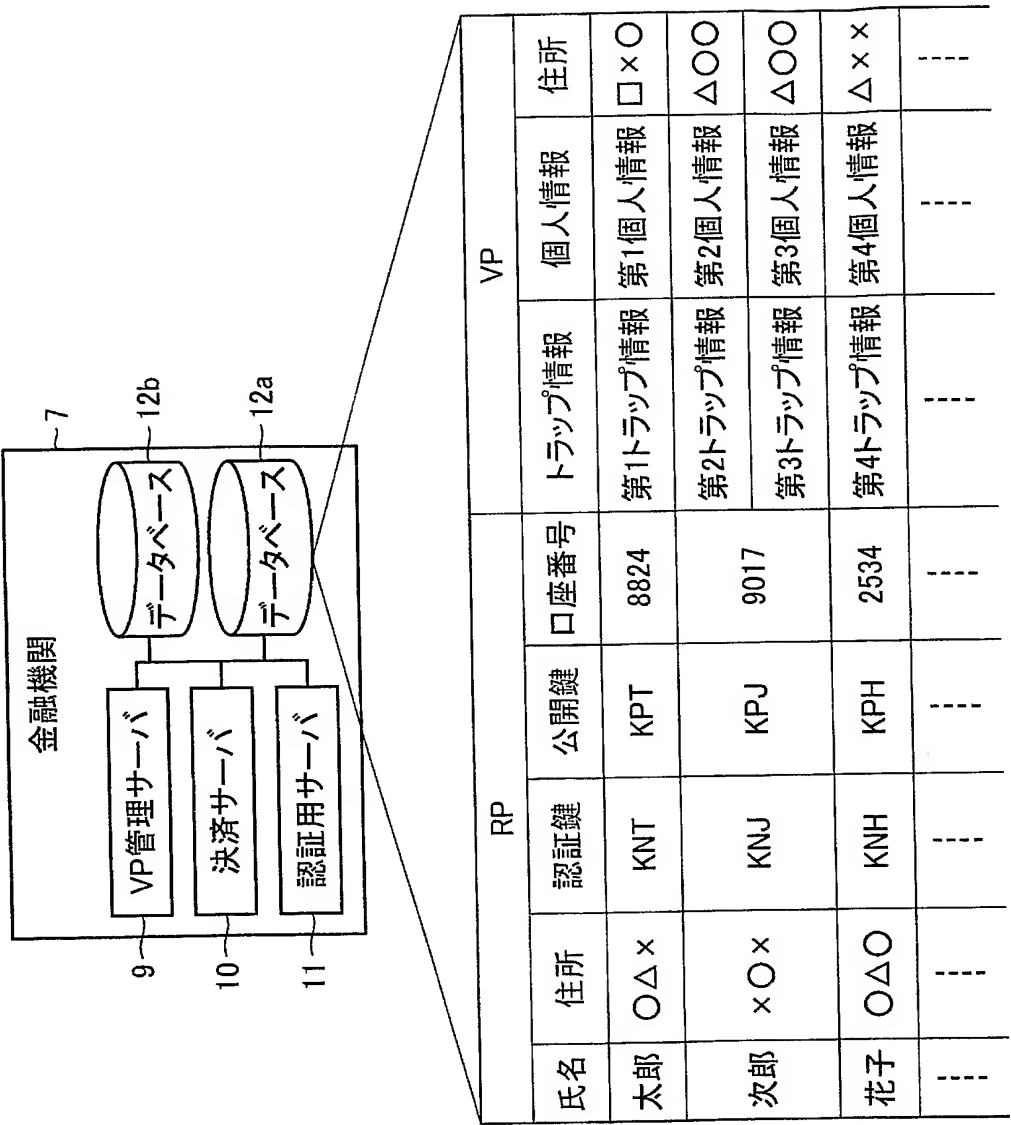
30 ブラウザフォン、7 金融機関、50 XMLストア、12a データベース、2 コンビニエンスストア、19V VP用 I C 端末、26 EEPROM、194 EEPROM、1 形態装置、1a セキュリティ用の R F I D タグ、110 コンデンサ、206 決済用の通過ゲート、80 メールサーバ、82 業社側端末、85 Eメール。

【書類名】 図面

【図 1】



【図 2】



【図 3】

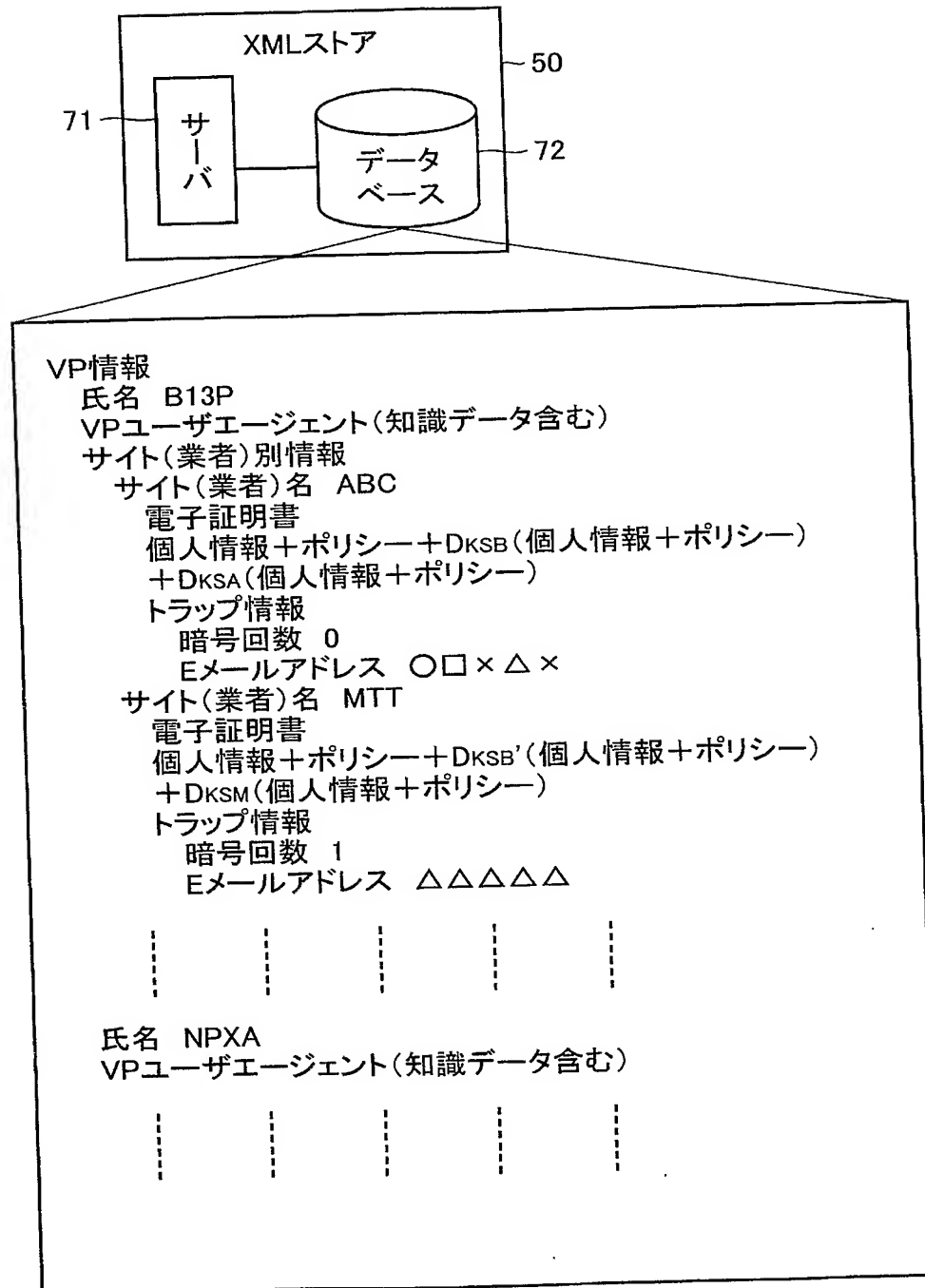
第1トラップ情報	サイト名 (業者名)	ABC	MTT	MEC	-----
	氏名	B13P	E(B13P)	E <sup>2</sup> (B13P)	-----
	公開鍵	KPB	KPB'	KPB''	-----
	Eメール アドレス	○□×△×	△△△△△	△△△△△	-----
	バーチャル 口座番号	2503	E(2503)	E <sup>2</sup> (2503)	-----
	バーチャル クレジット番号	9145	E(9145)	E <sup>2</sup> (9145)	-----
第2トラップ情報	サイト名 (業者名)	AMZ	RAK	ASK	-----
	氏名	NPXA	E(NPXA)	E <sup>2</sup> (NPXA)	-----
	公開鍵	KPN	KPN'	KPN''	-----
	Eメール アドレス	××○△□	△△△△△	△△△△△	-----
	バーチャル 口座番号	3541	E(3541)	E <sup>2</sup> (3541)	-----
	バーチャル クレジット番号	3288	E(3288)	E <sup>2</sup> (3288)	-----
⋮	⋮	⋮	⋮	⋮	

【図 4】

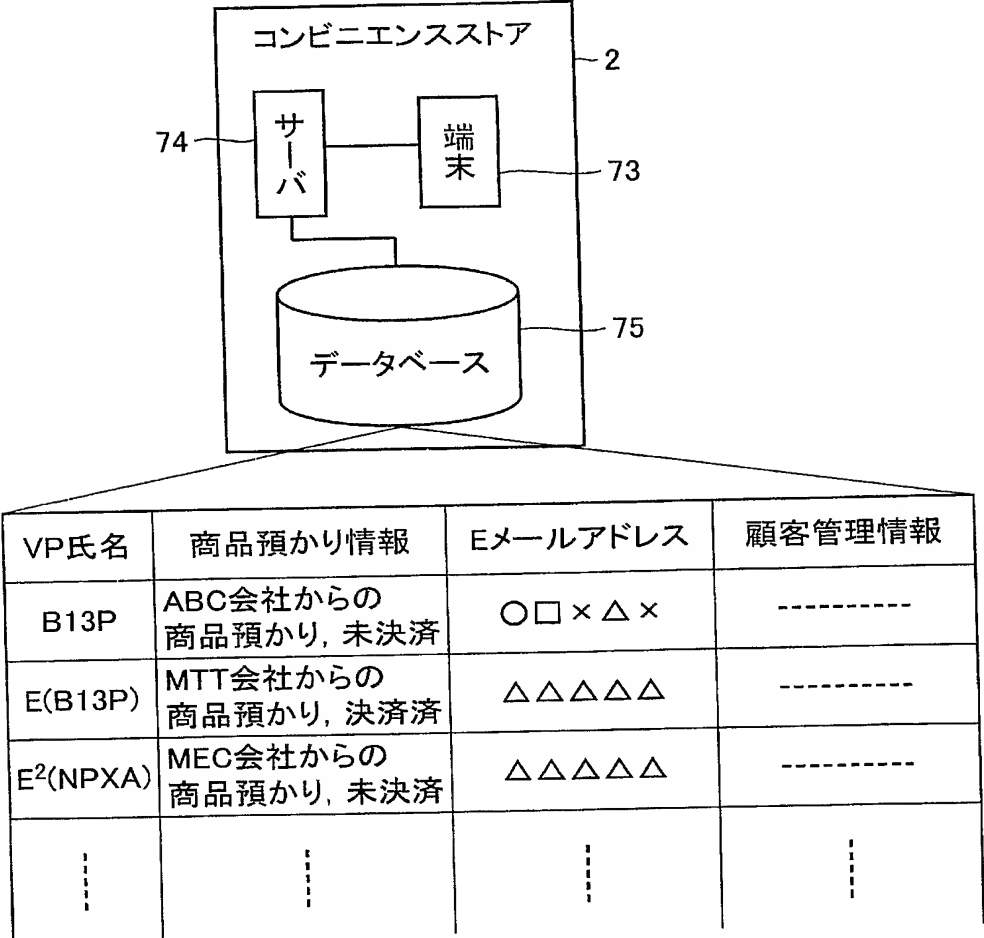
	個人情報A	個人情報B	-----
第1個人情報	〇〇△+Dks(〇〇△)	××△+Dks(××△)	-----
第2個人情報	△〇〇+Dks(△〇〇)	△××+Dks(△××)	-----
第3個人情報	〇△〇+Dks(〇△〇)	×△×+Dks(×△×)	-----
第4個人情報	△〇△+Dks(△〇△)	△×△+Dks(△×△)	-----
⋮	⋮	⋮	



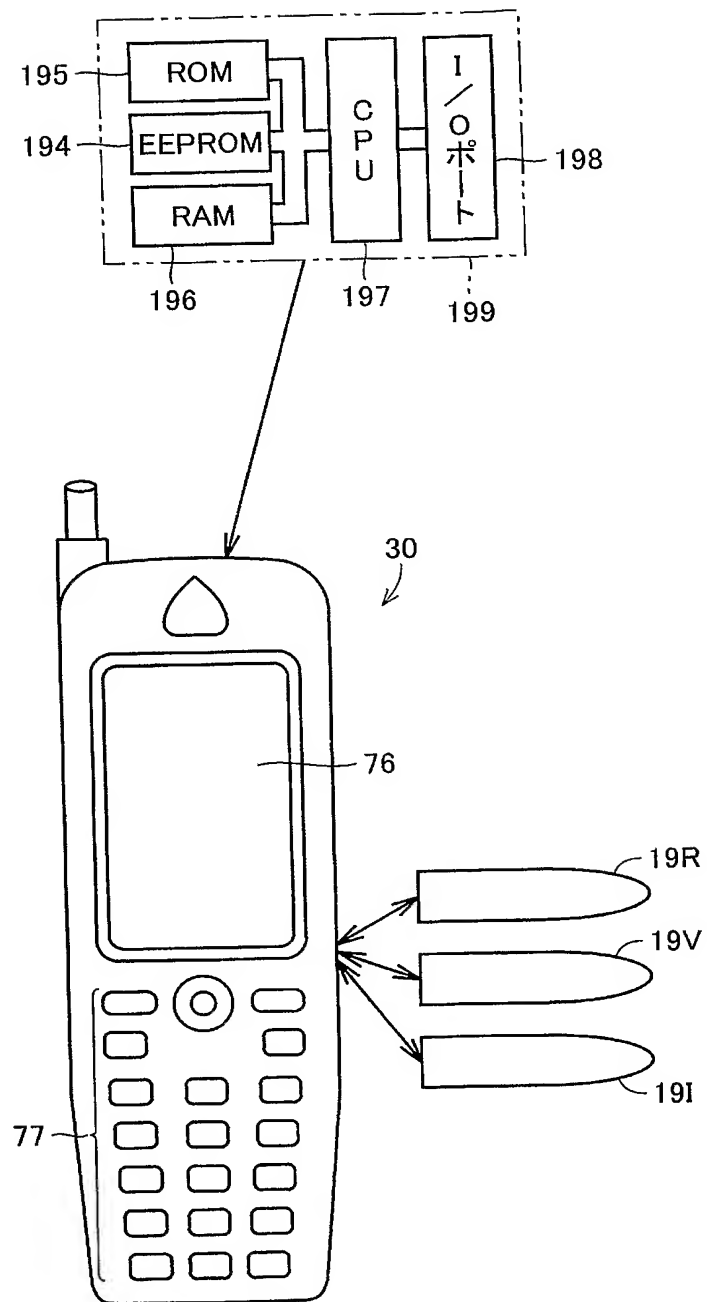
【図 5】



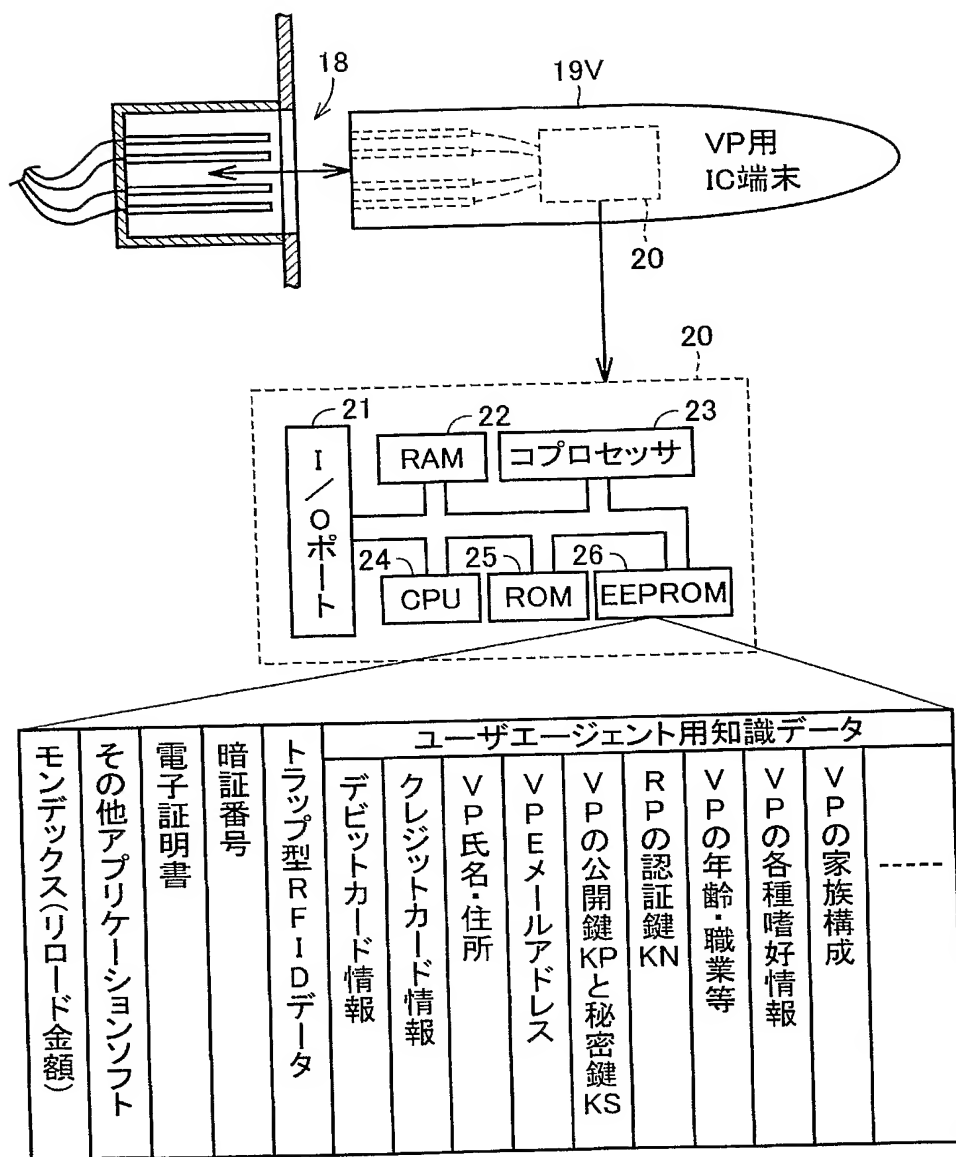
【図 6】



【図 7】



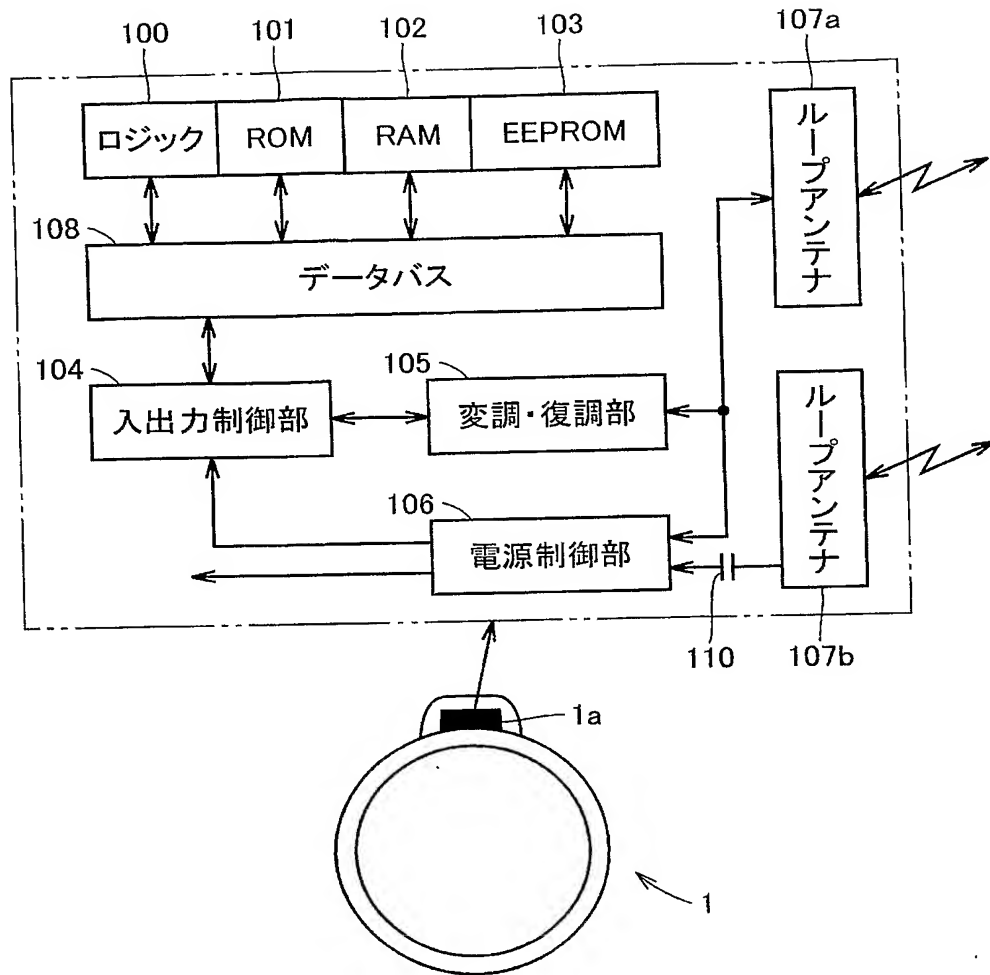
【図 8】



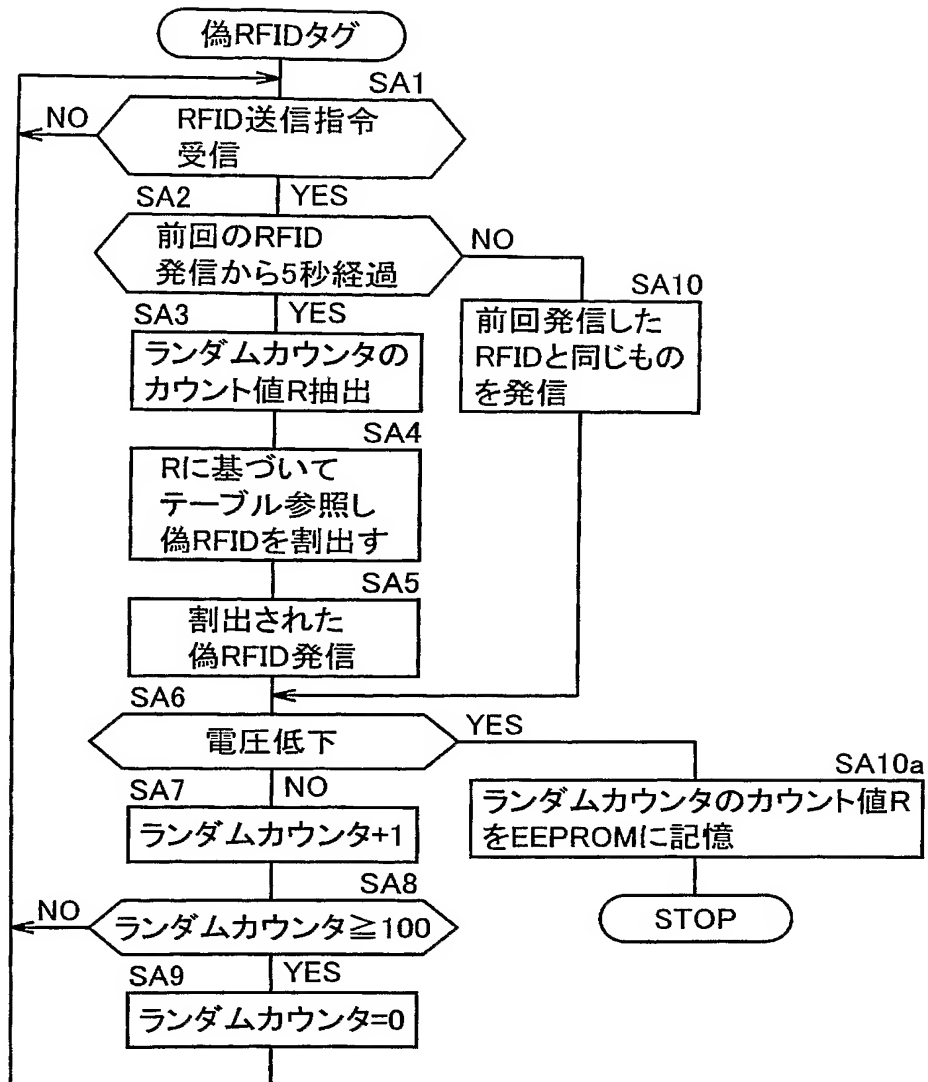
【図 9】

トラップ型RFIDデータ		
VP氏名	トラップ型RFID	業者名
B13P	abc,hij,amz,rak,...	ABC,HIJ,AMZ...
E(B13P)	mtt	MTT
E <sup>2</sup> (B13P)	mec	MEC
E <sup>3</sup> (B13P)	ktt	KTT
⋮	⋮	⋮

【図 10】



【図 11】





【図 12】

(a)

R	0～39	40～54	55～69	70～84	85～99
RFID	820493176	730854709	813926081	791405731	835406912

(b)

R	0～39	40～54	55～69	70～84	85～99
RFID1	831709281	793102792	814358231	840526390	751052891
RFID2	779203980	809132041	849137655	789182509	850021934
RFID3	839093127	749084765	788015233	850139767	802049344
RFID4	740980346	808645210	779288401	750561234	766104988

(c)

R	0～39	40～54	55～69	70～84	85～99
RFID1	799804511	717950841	899893020	879010300	700913561
RFID2	779203980	709130241	749182655	889121509	750021214
RFID3	839093127	849048765	888062233	750161767	702049319
RFID4	740980346	708642510	879264401	850561202	856104923

【図 13】

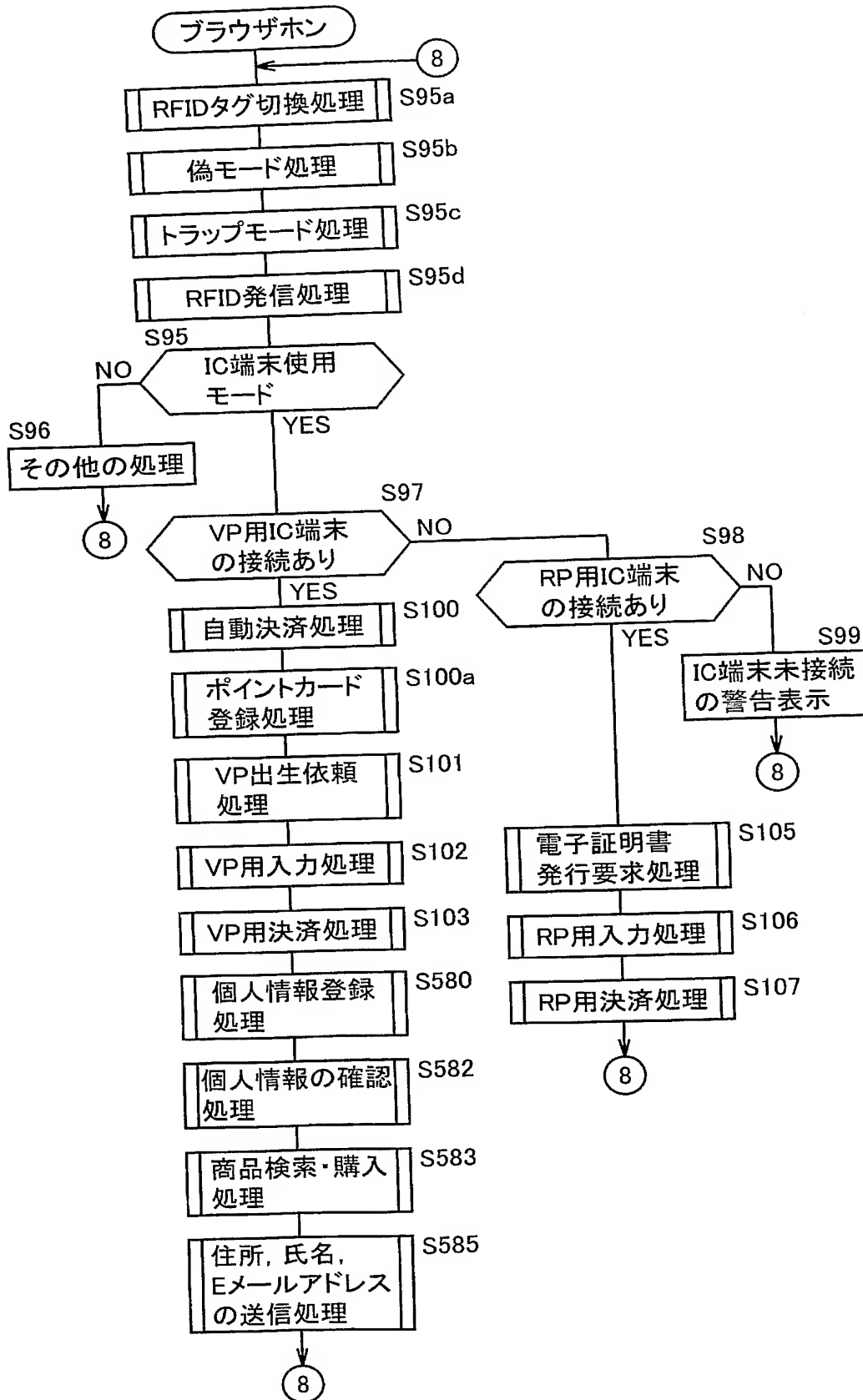
(a)

共通偽RFID	販売地域
820493176	千代田区
809207321	新宿区
831902845	渋谷区
§	§
798091320	右京区

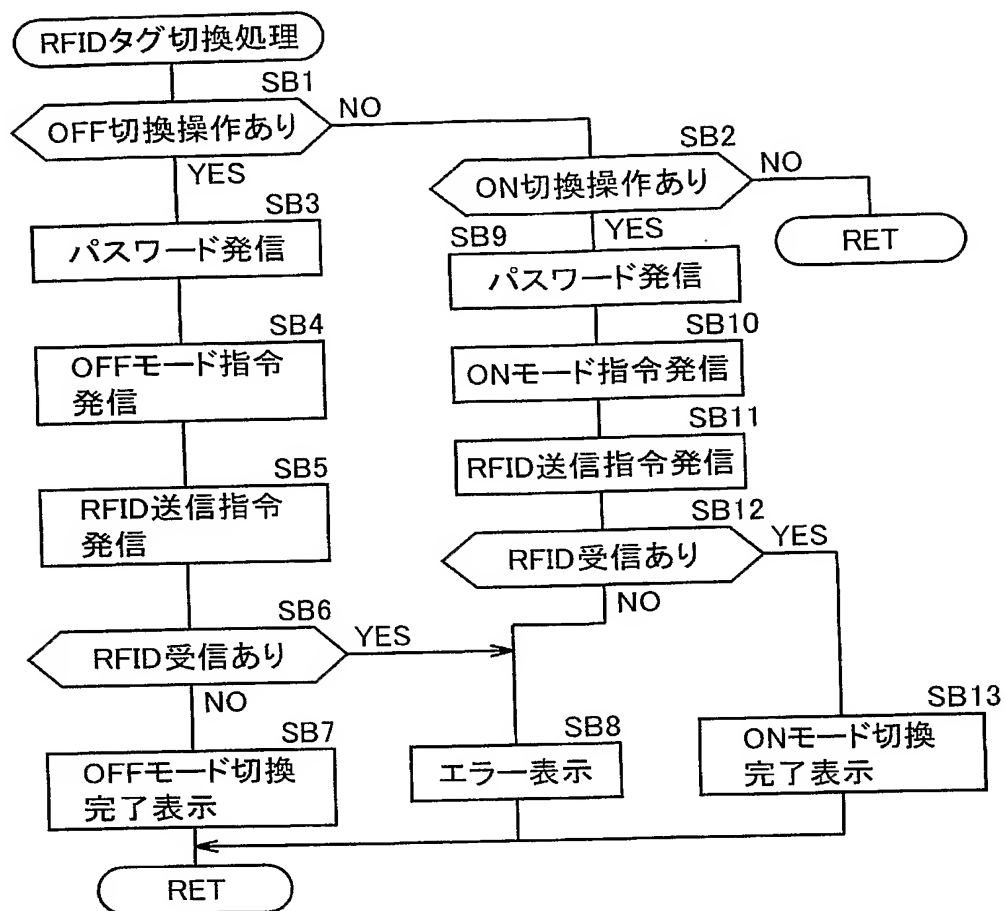
(b)

共通偽RFID	販売地域
779203980 839093127 740980346	千代田区
810391562 781529055 808892177	新宿区
§	§
788718955 845590329 822770945	右京区

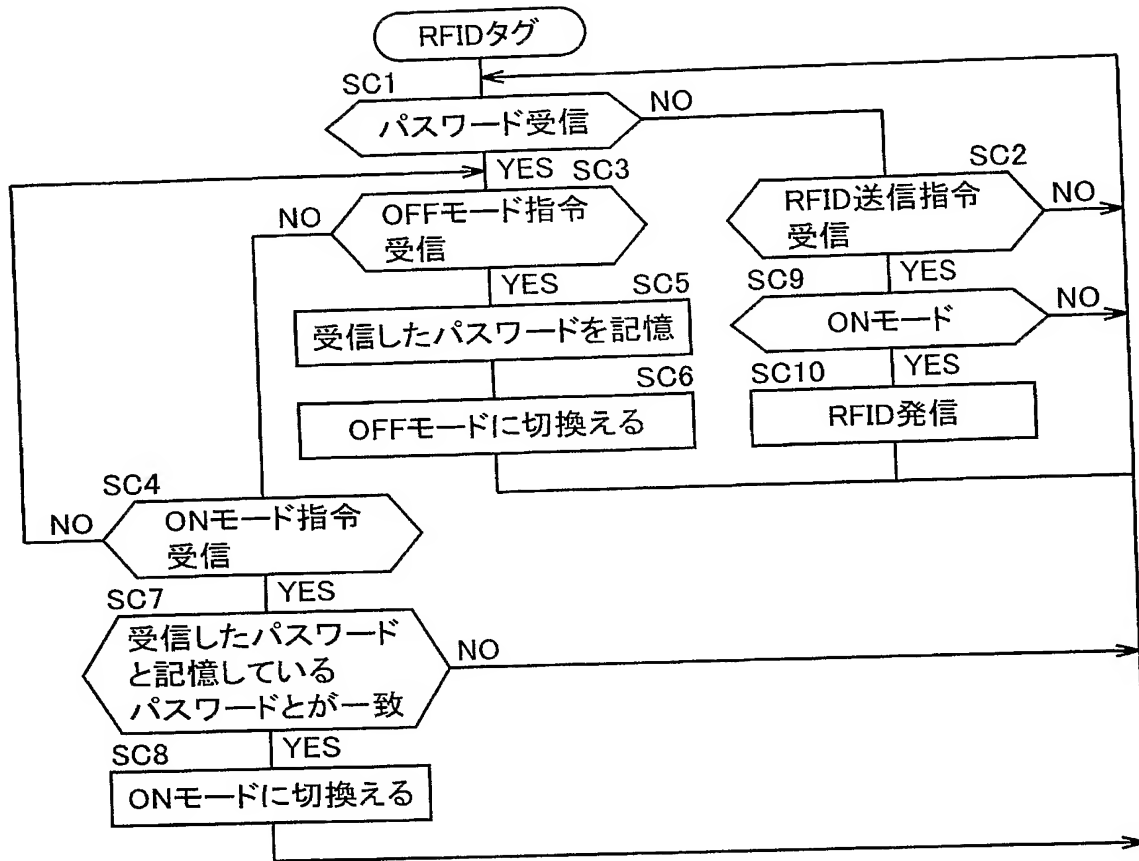
【図 14】



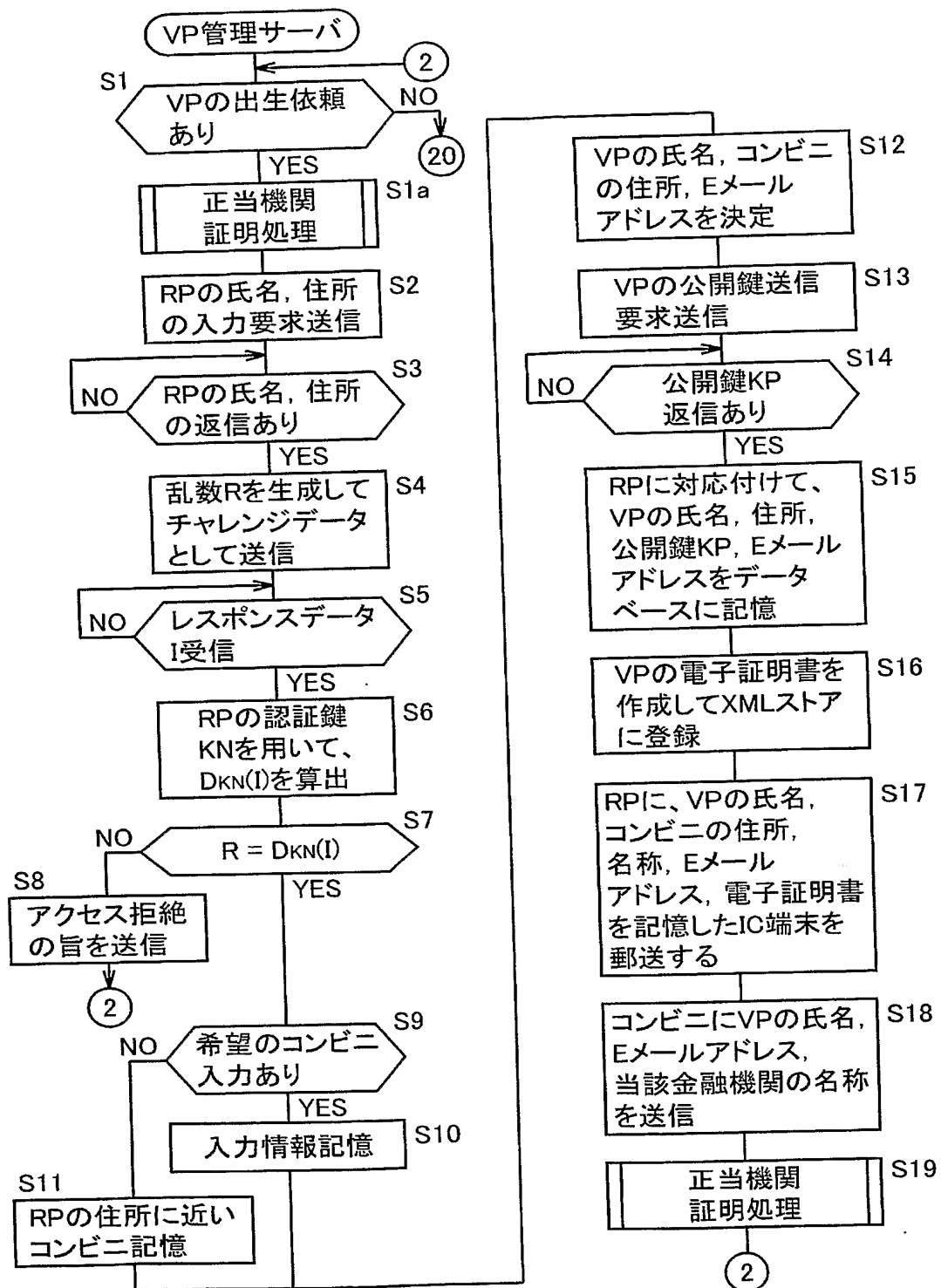
【図15】



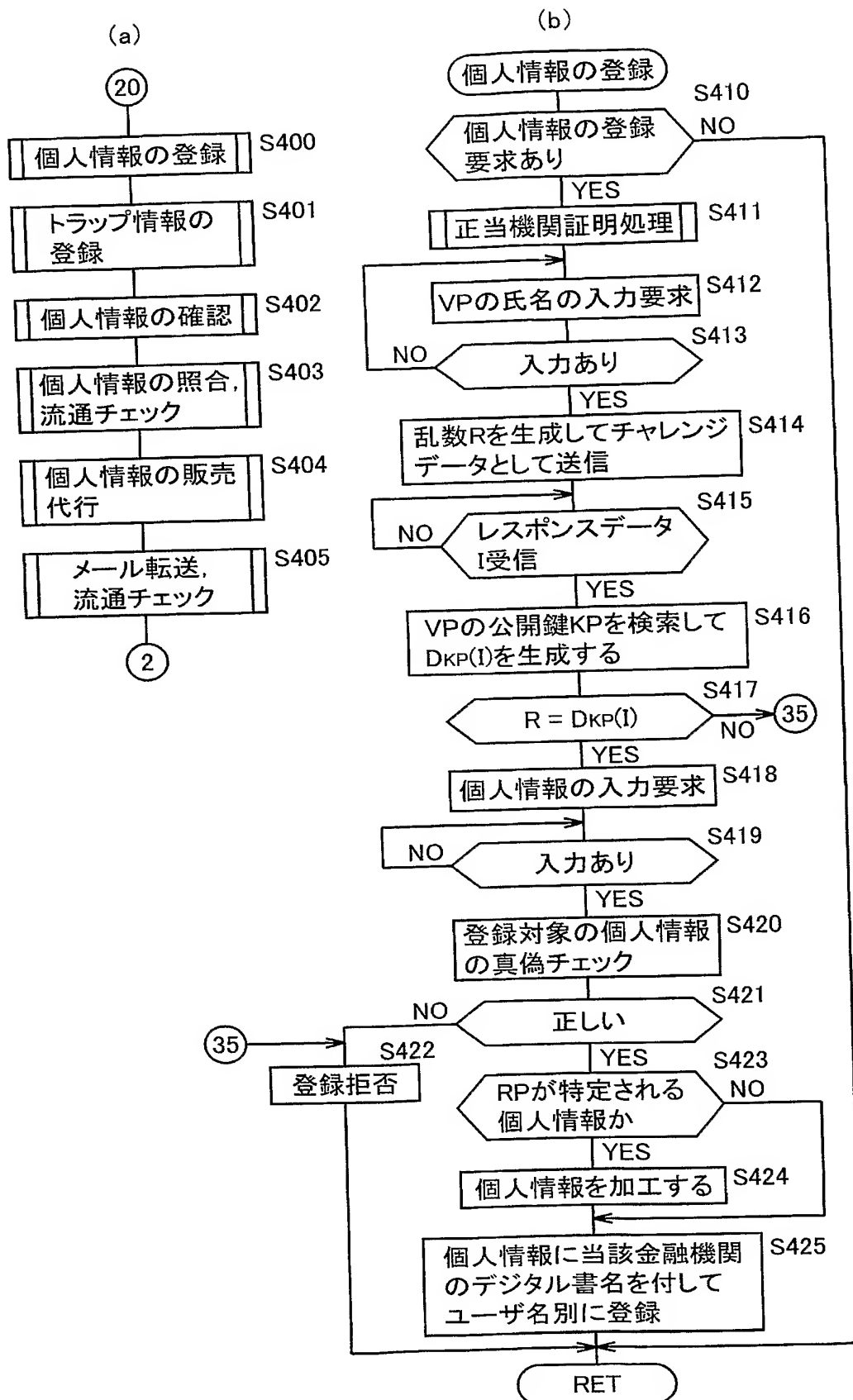
【図16】



【図17】

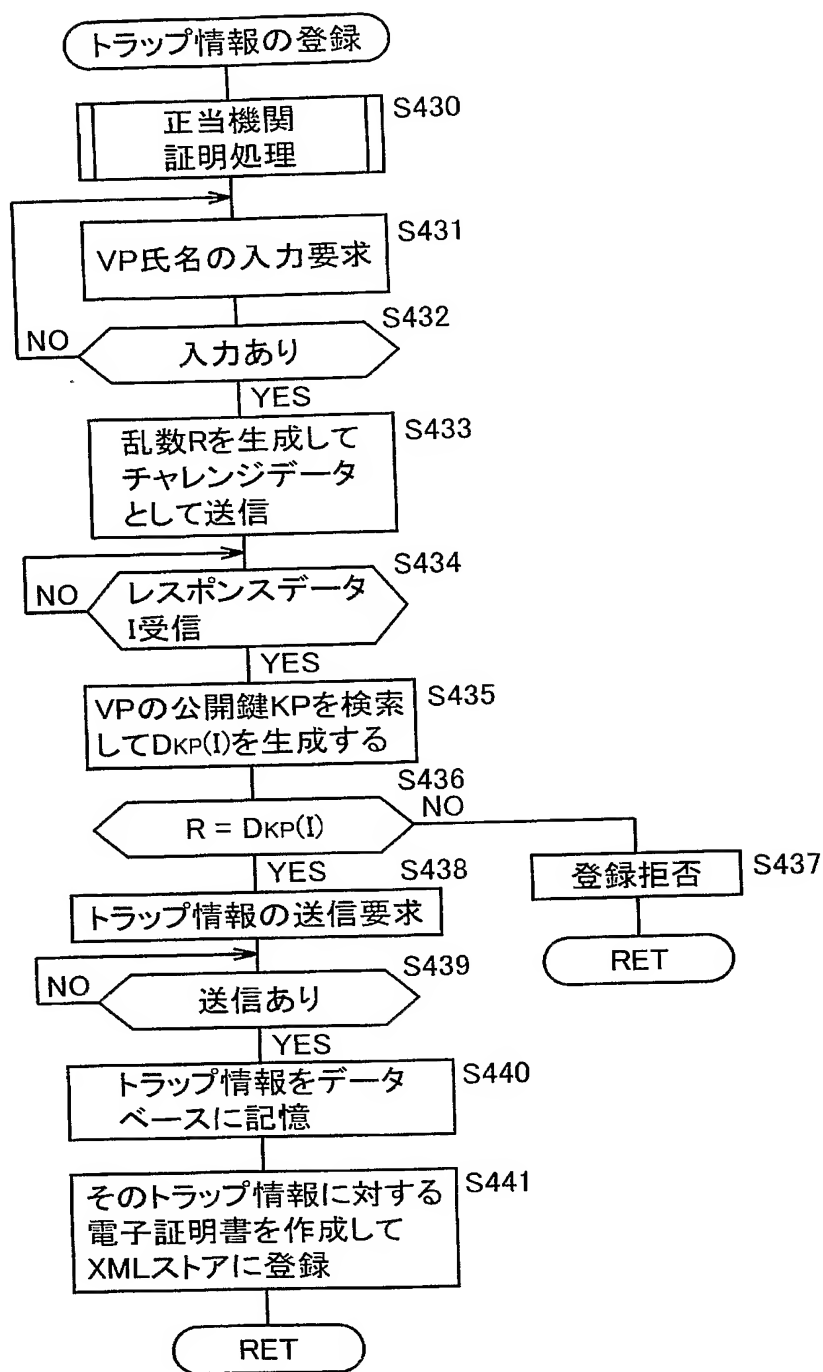


【図 18】

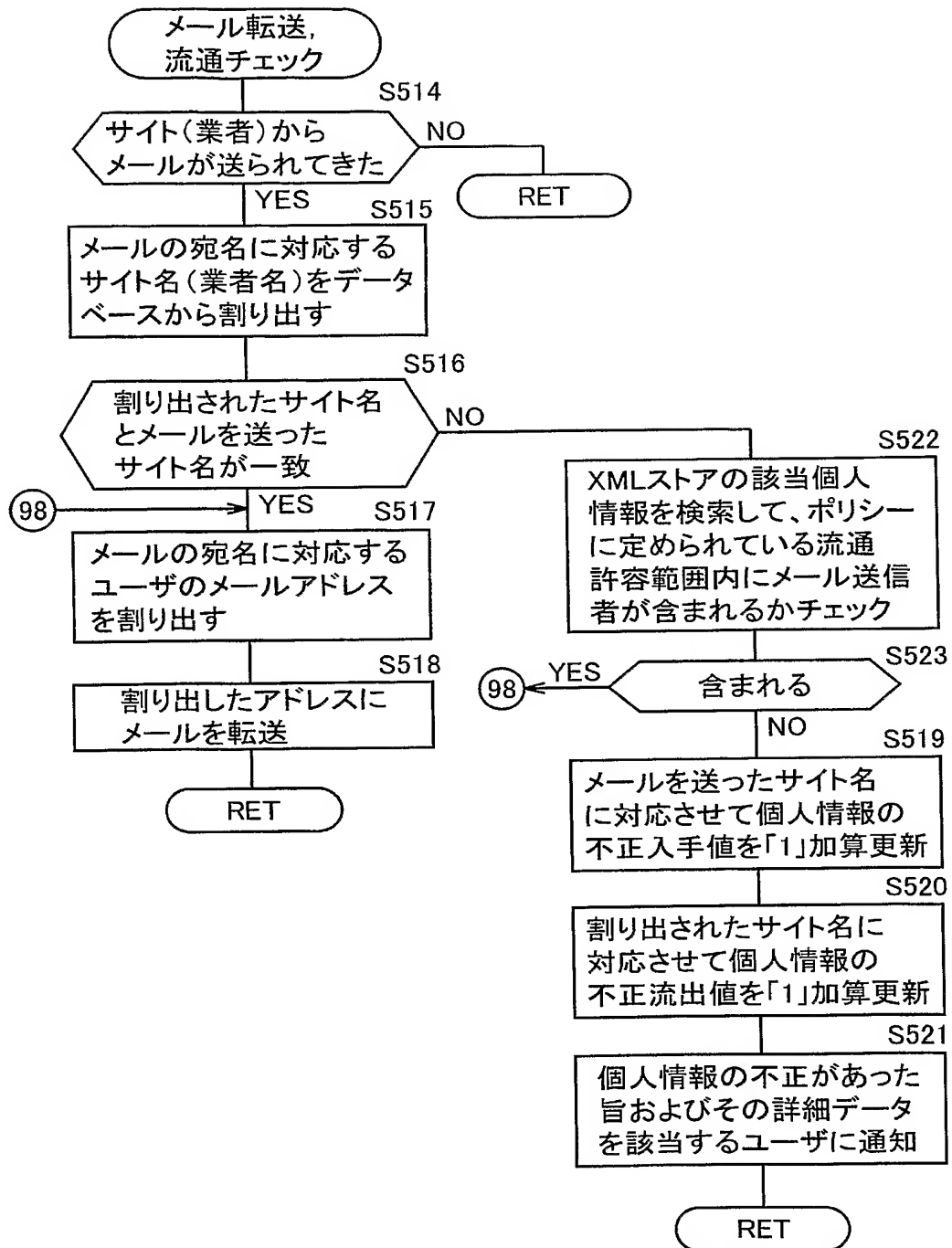




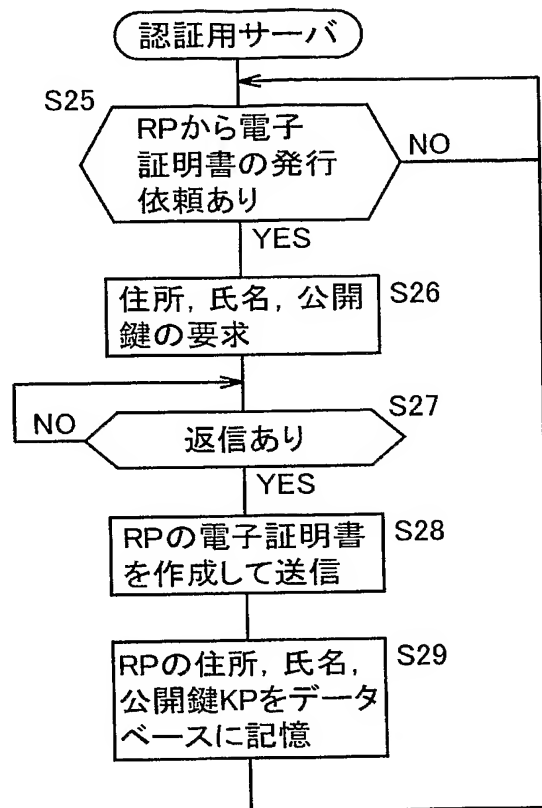
【図 19】



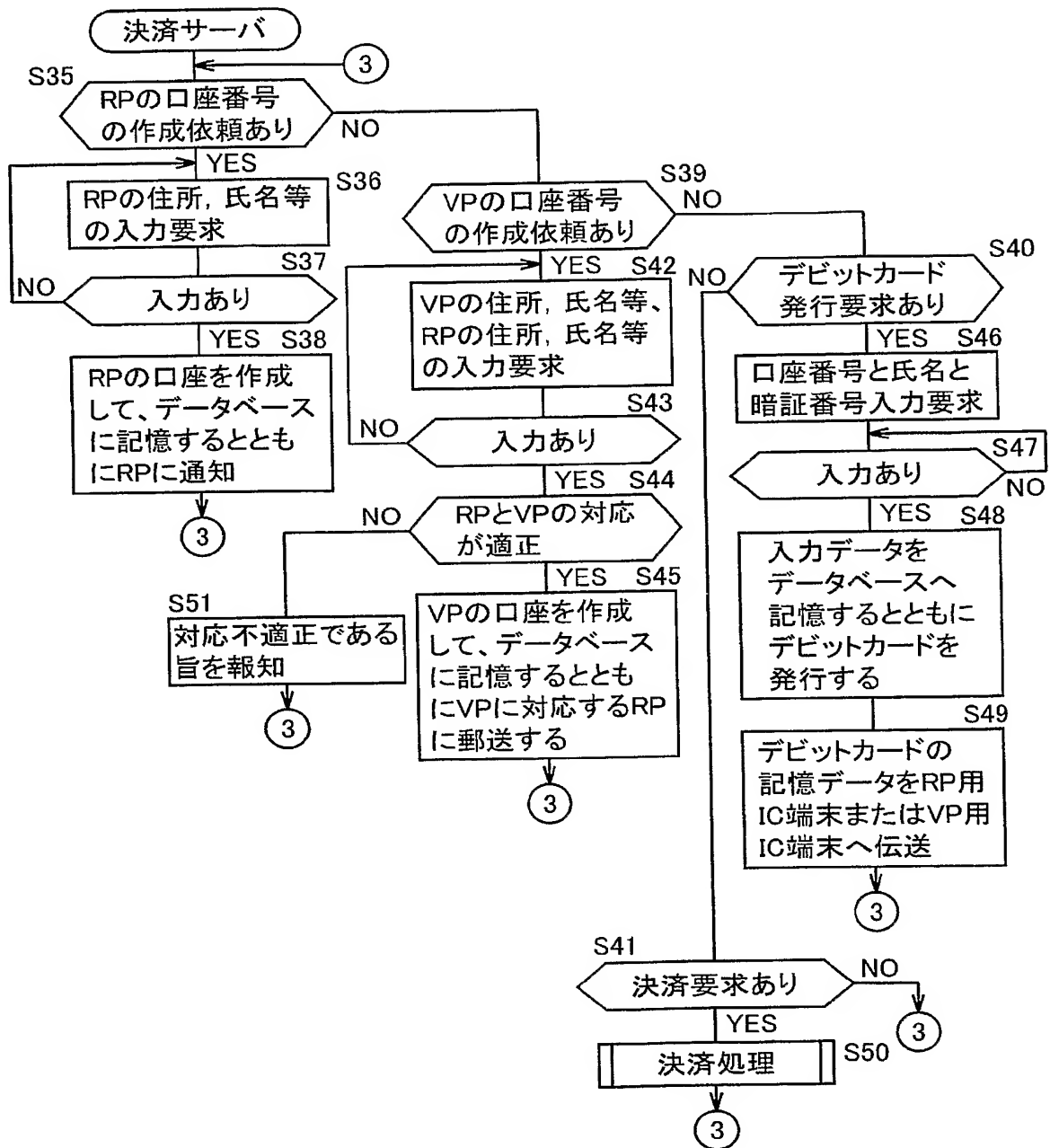
【図 20】



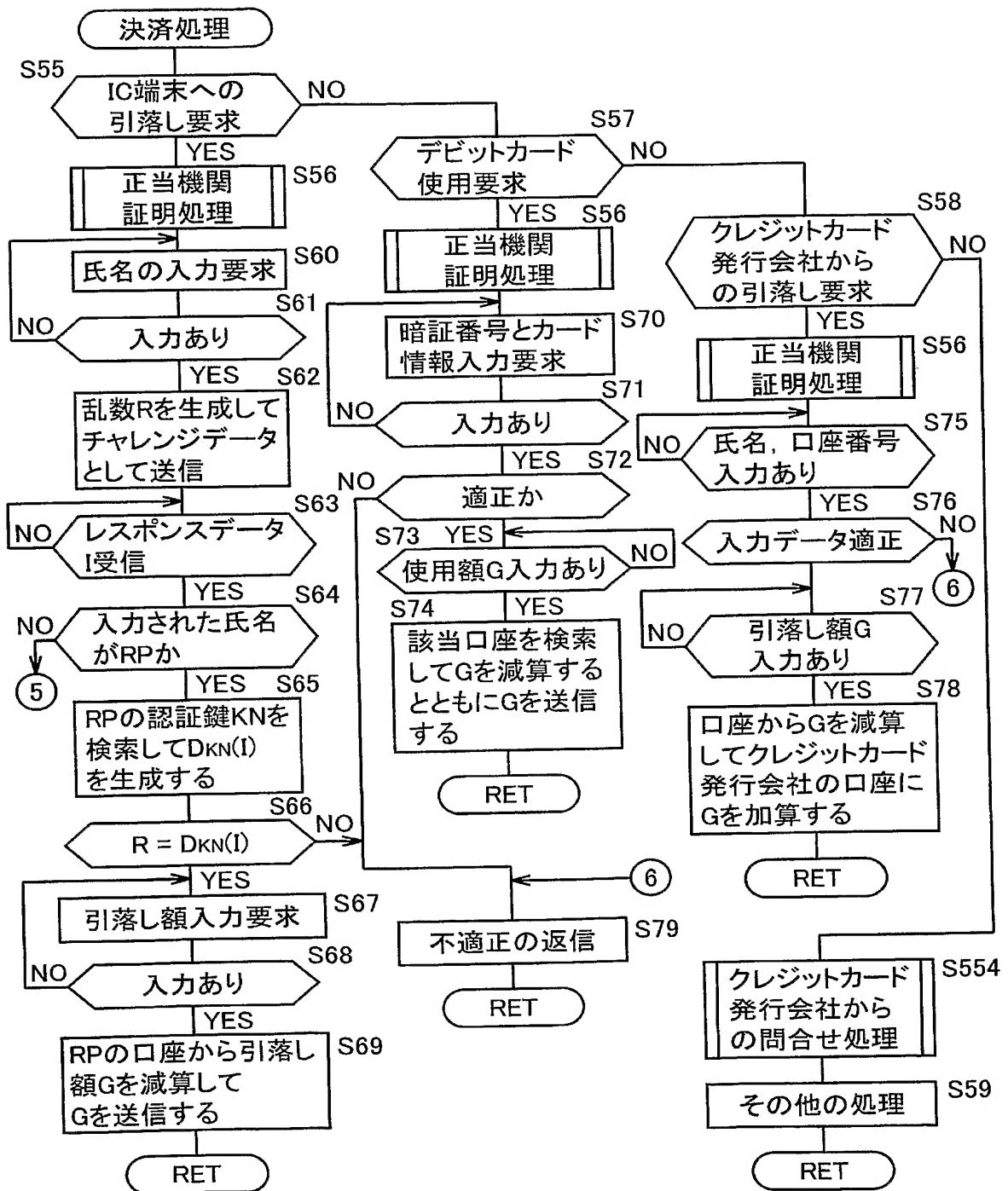
【図 21】



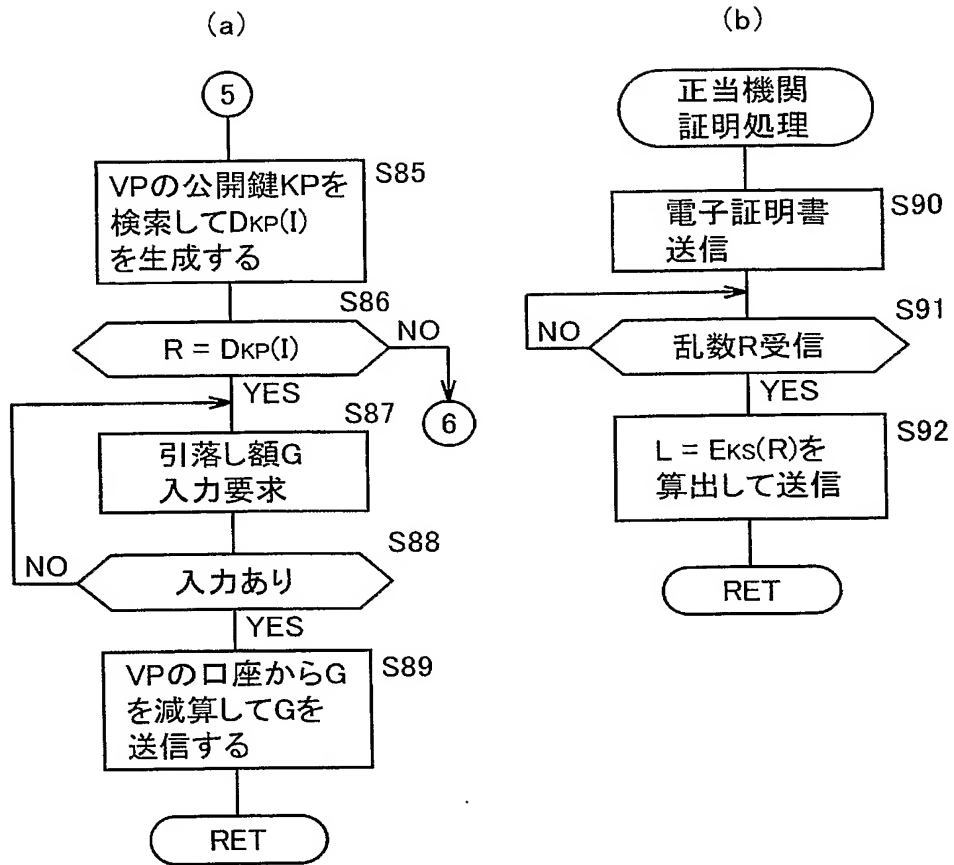
【図 22】



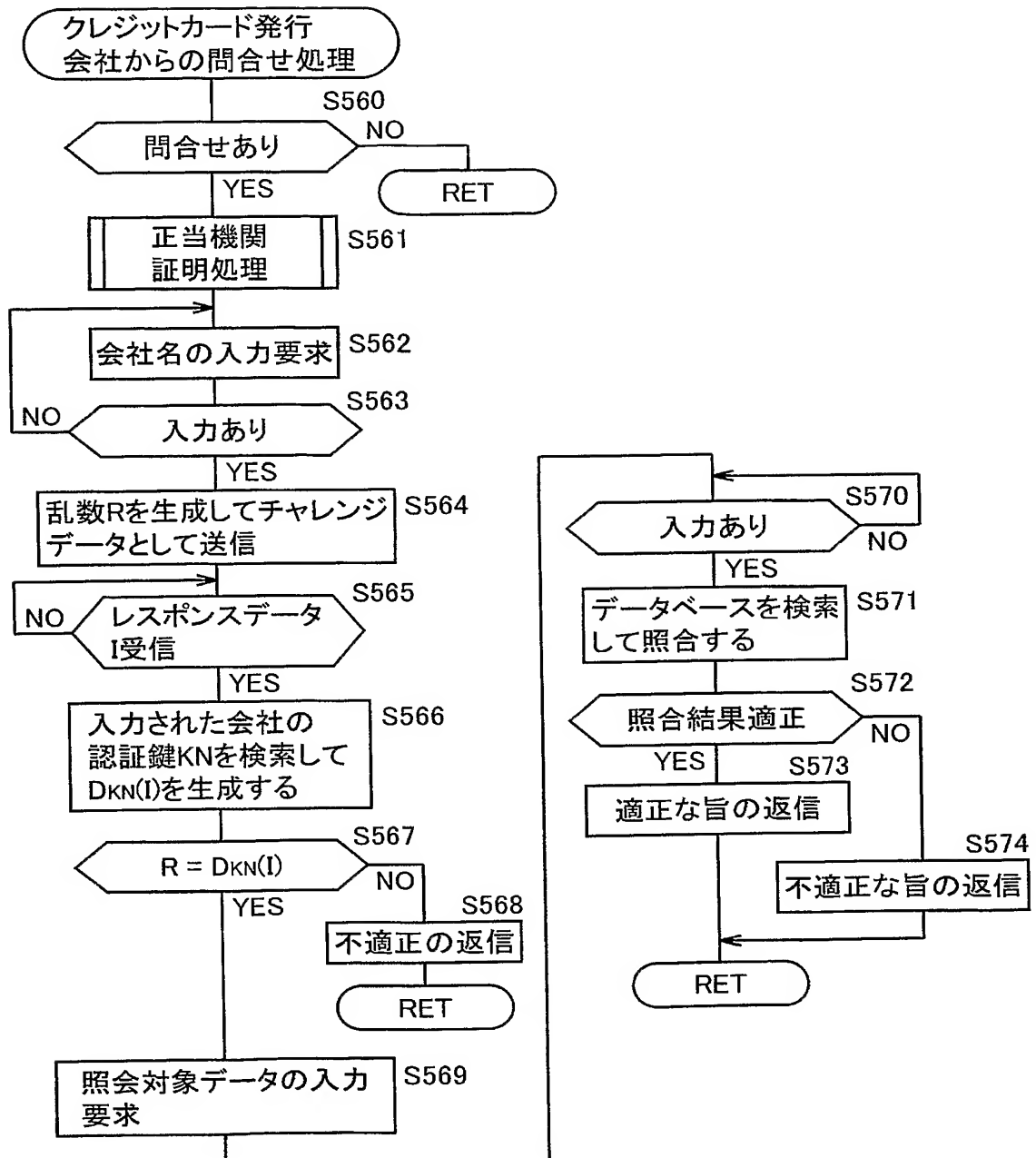
【図 23】



【図 24】

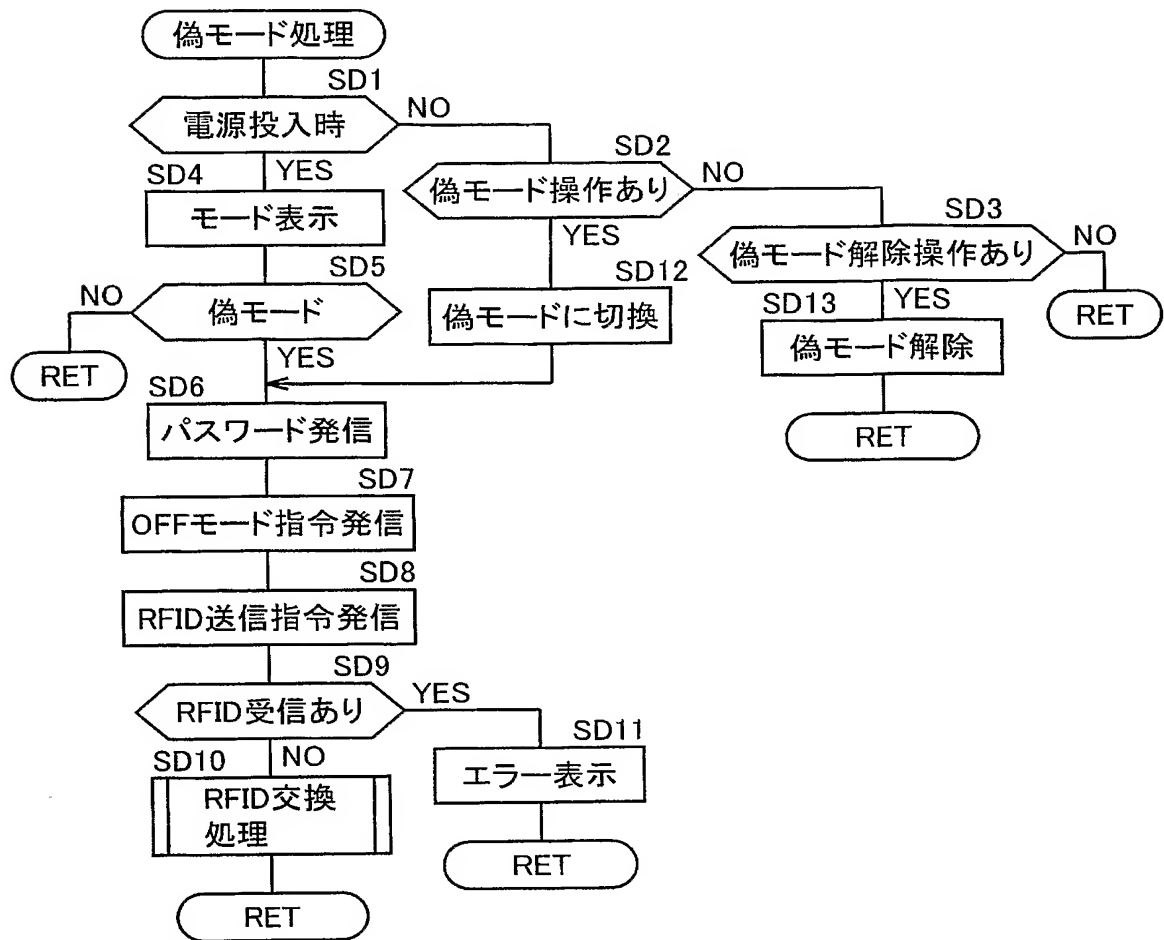


【図 25】

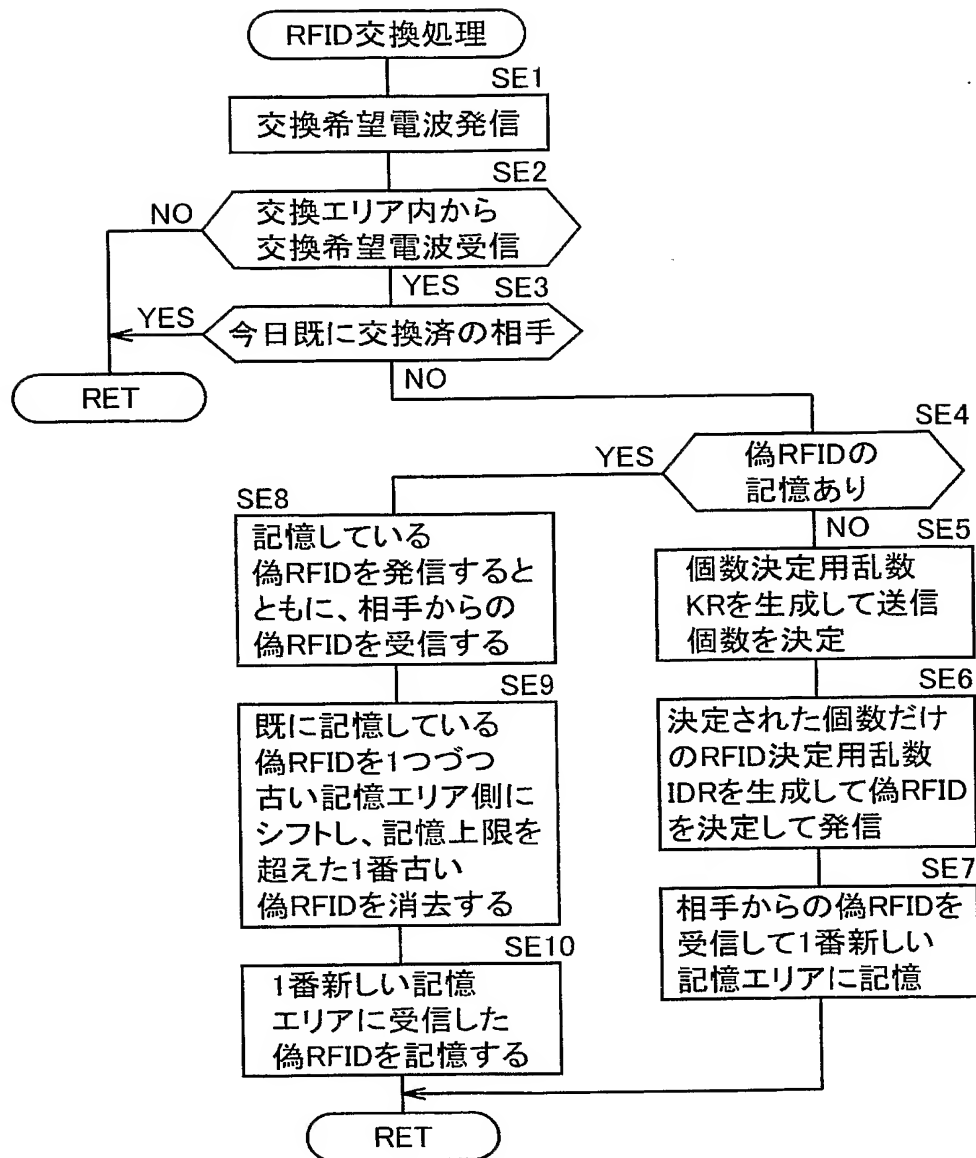




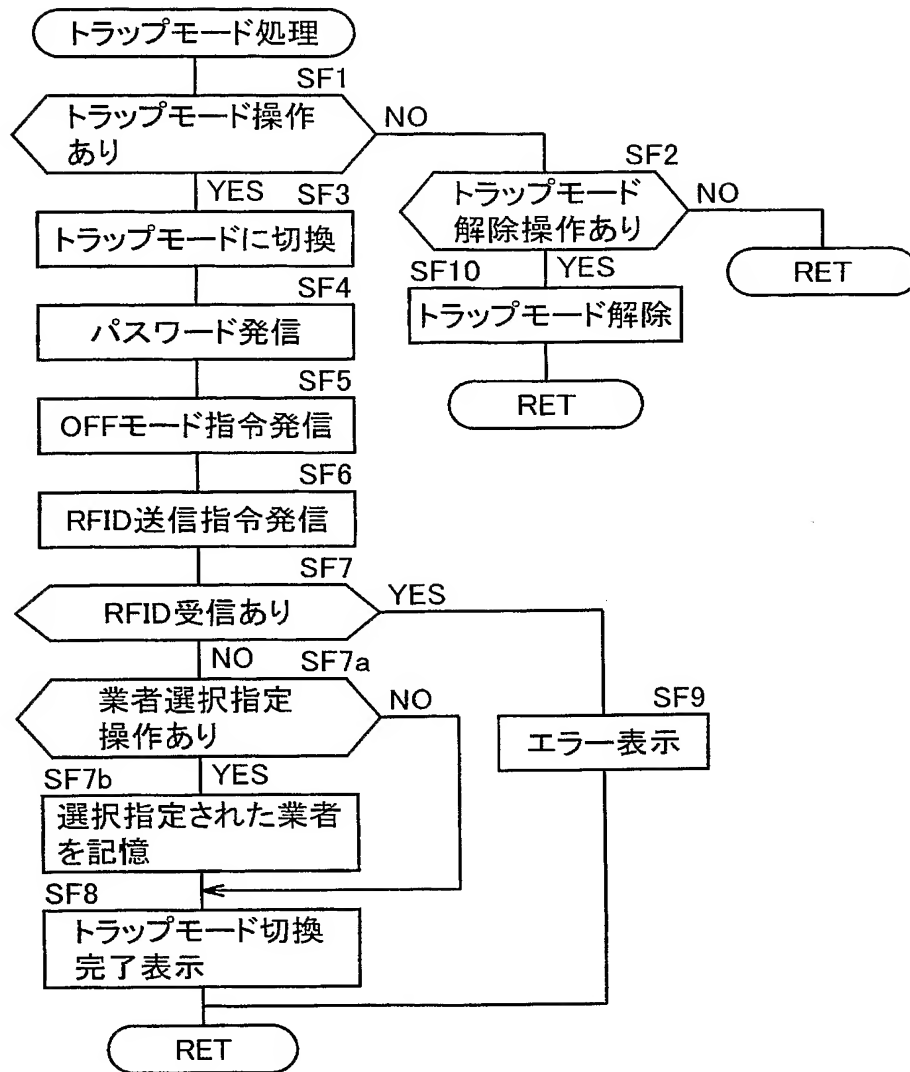
【図 26】



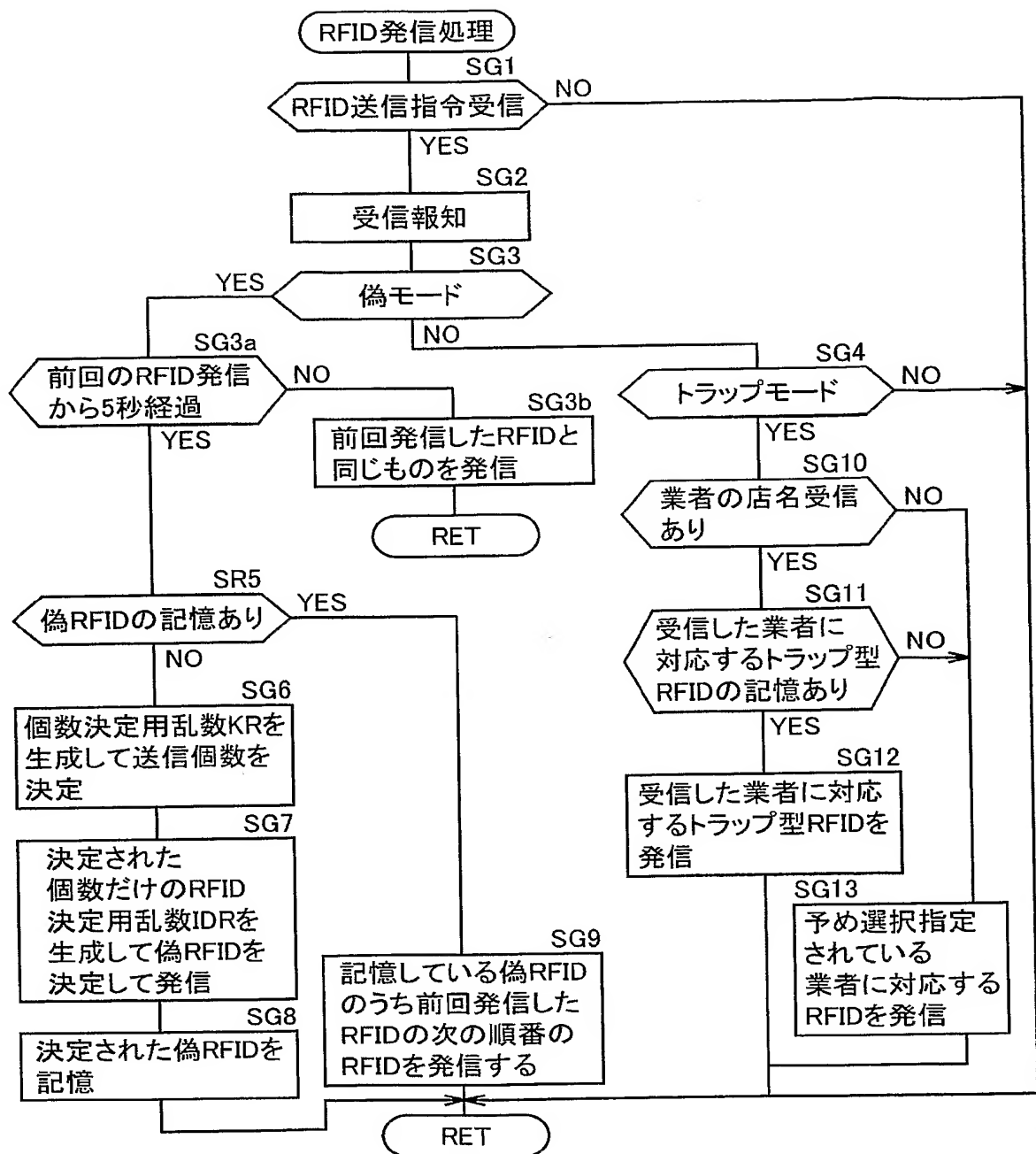
【図 27】



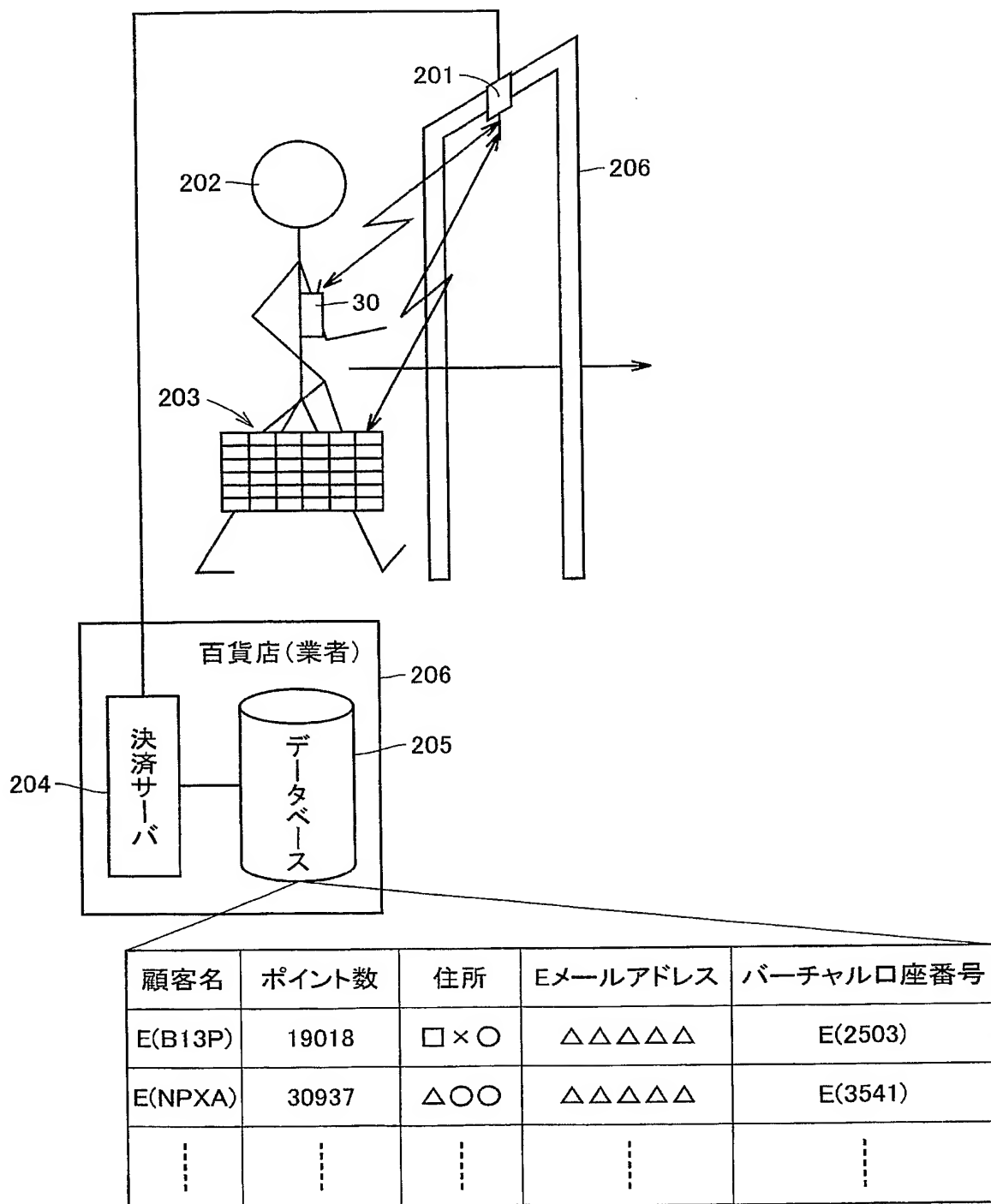
【図 28】



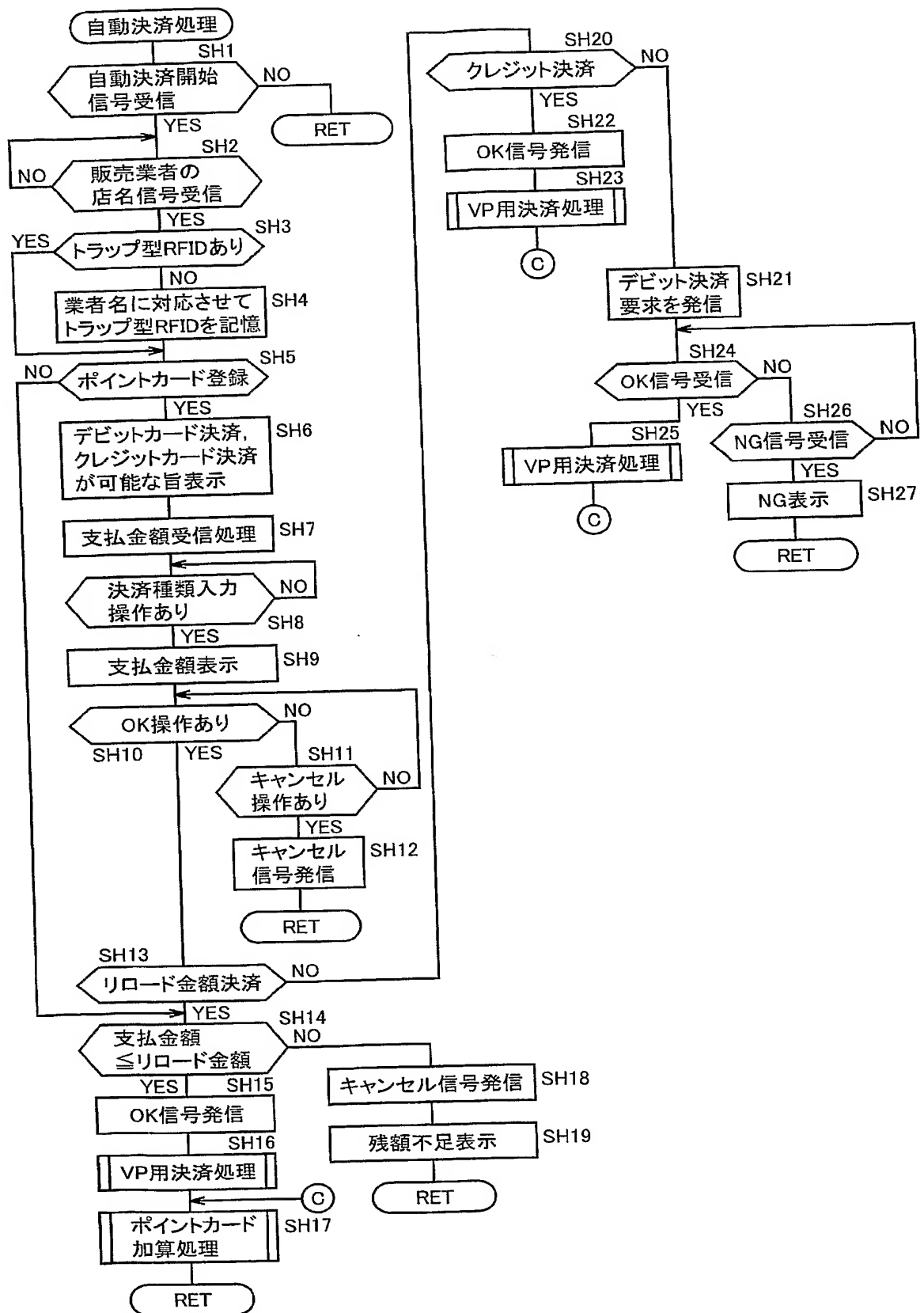
【図 29】



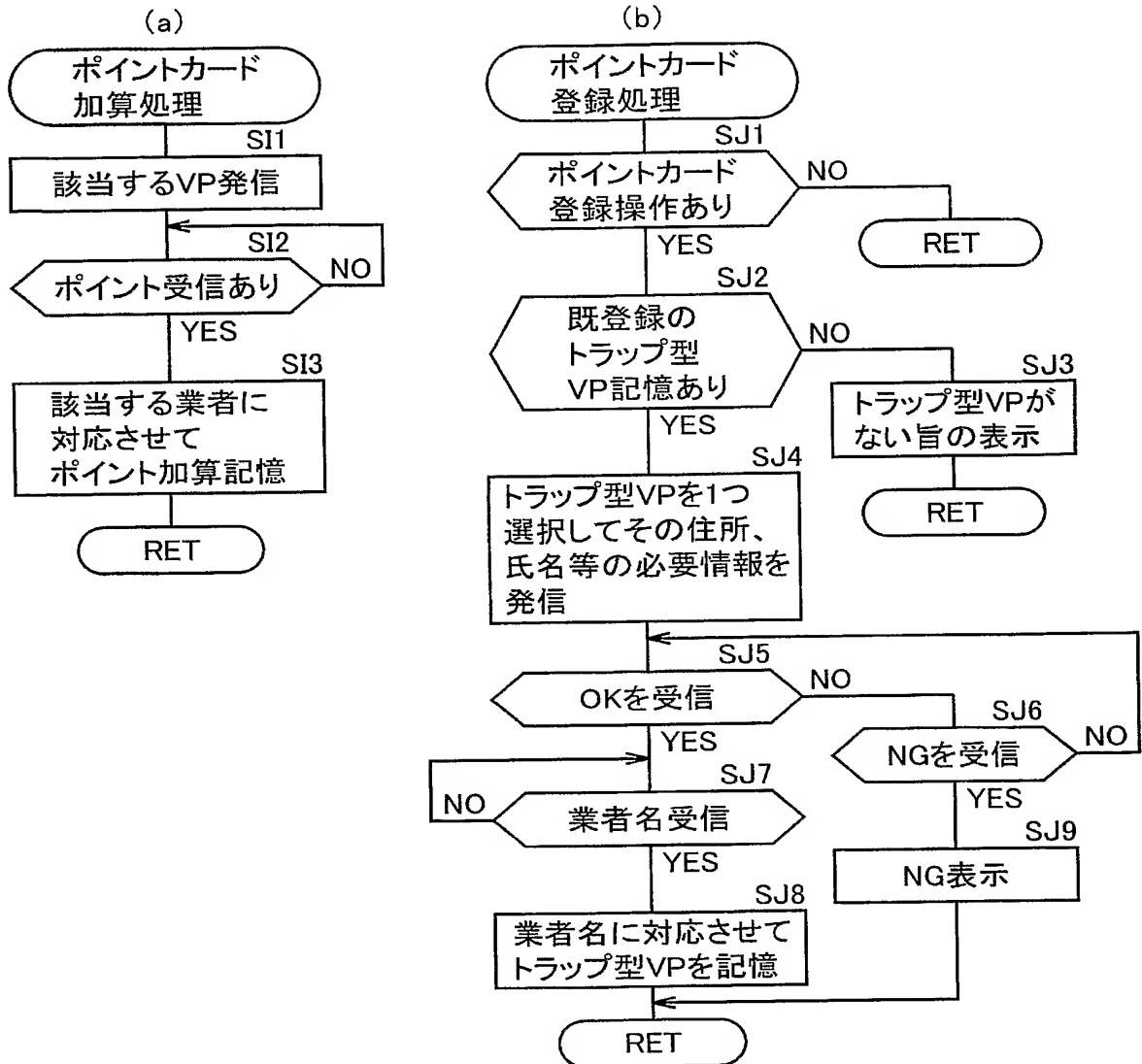
【図 30】



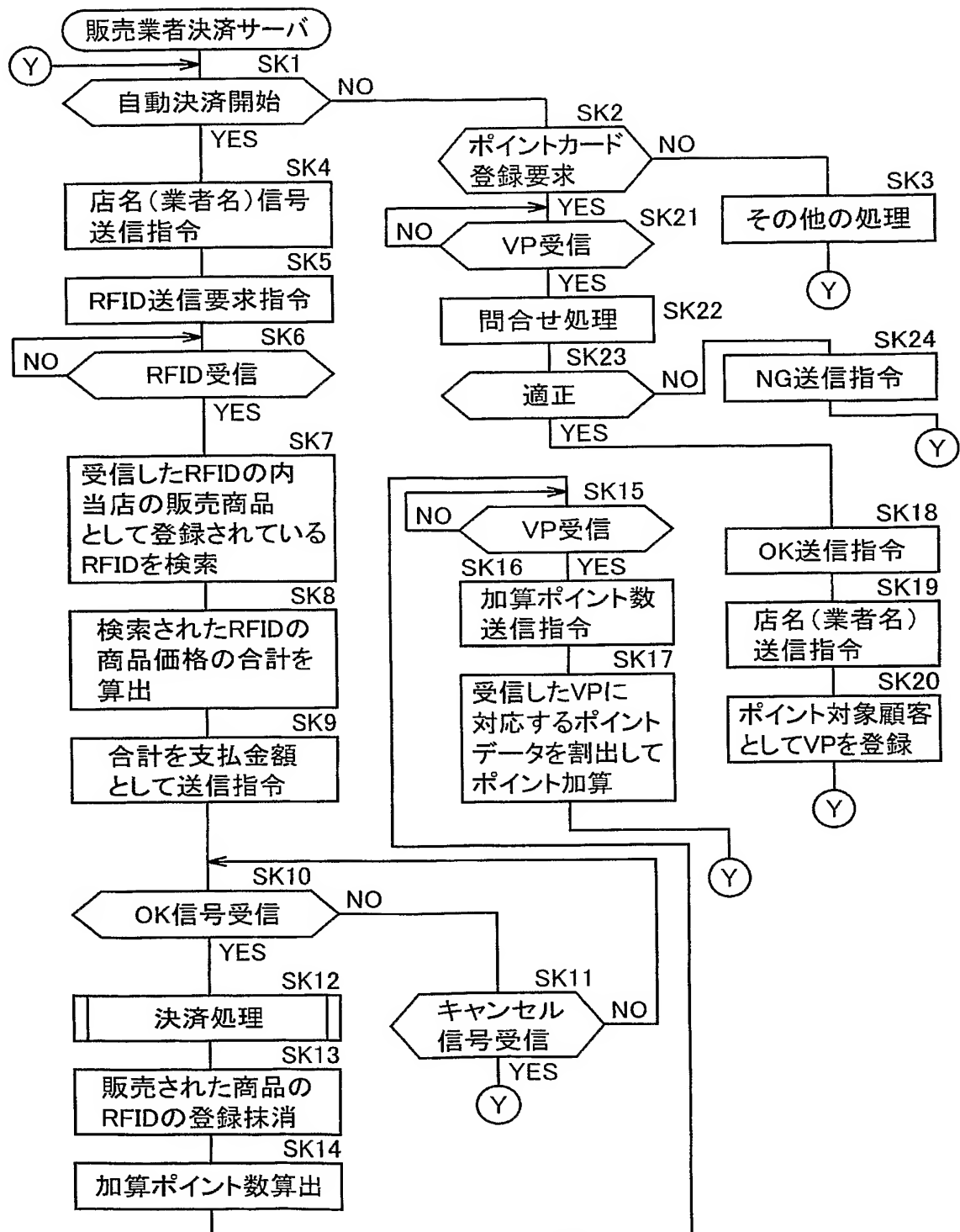
【図 31】



【図 3 2】

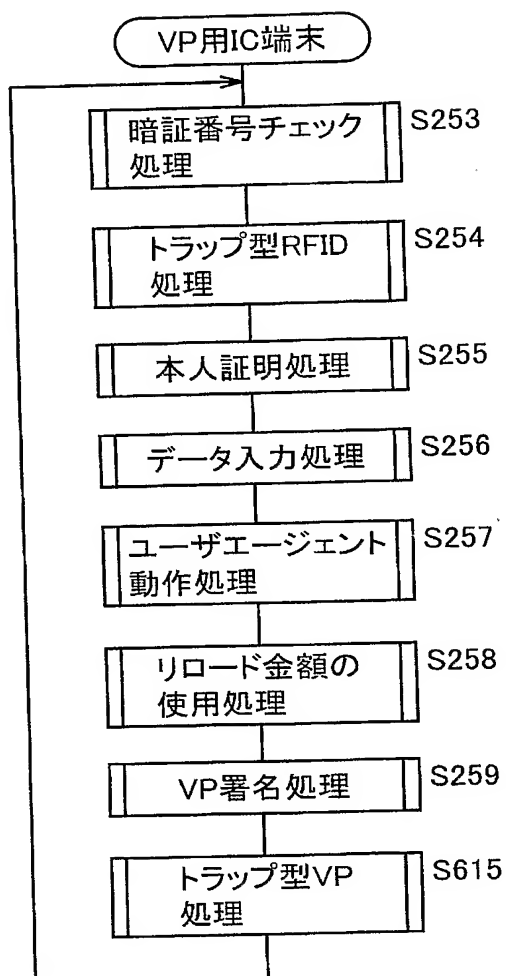


【図 33】

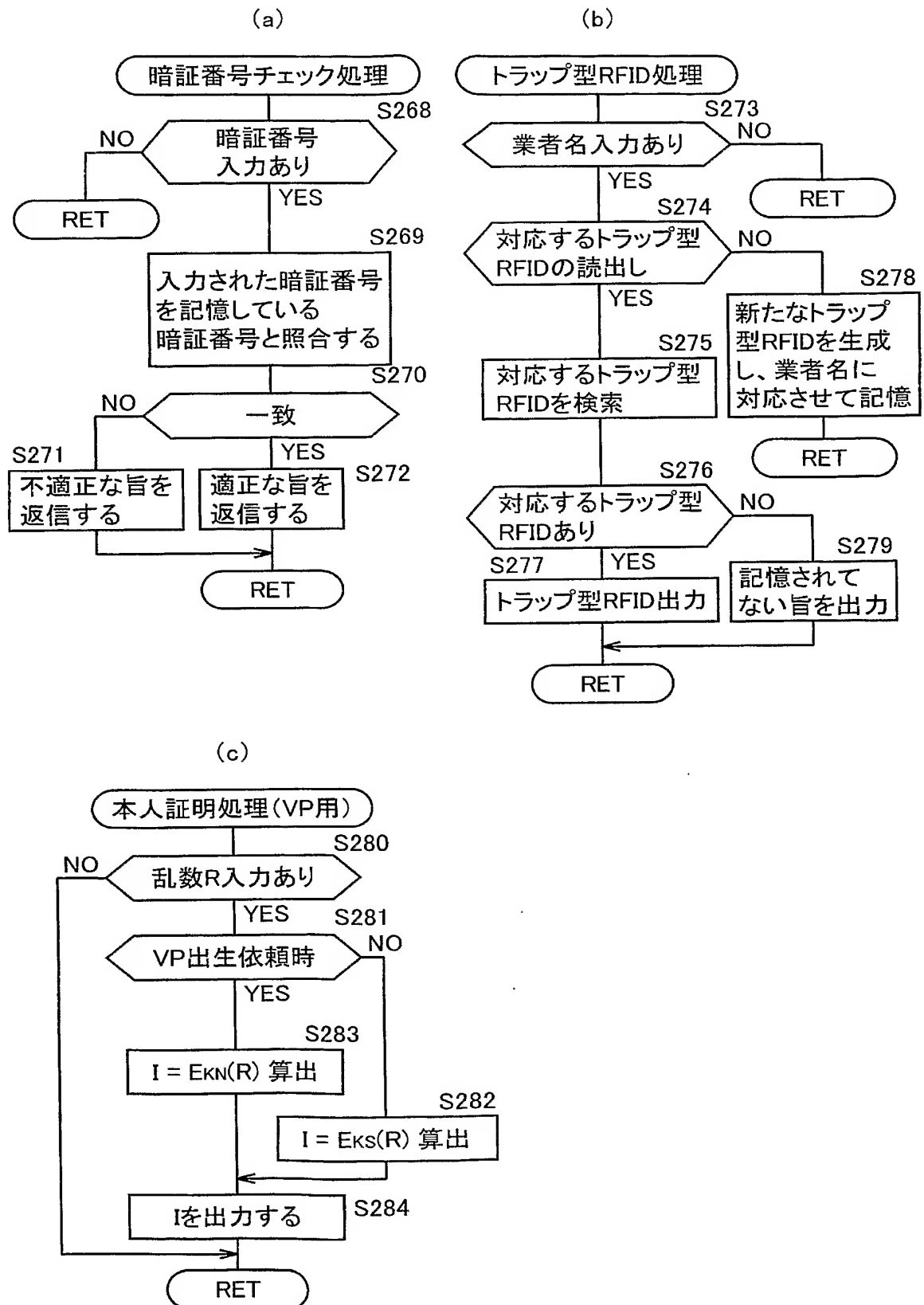




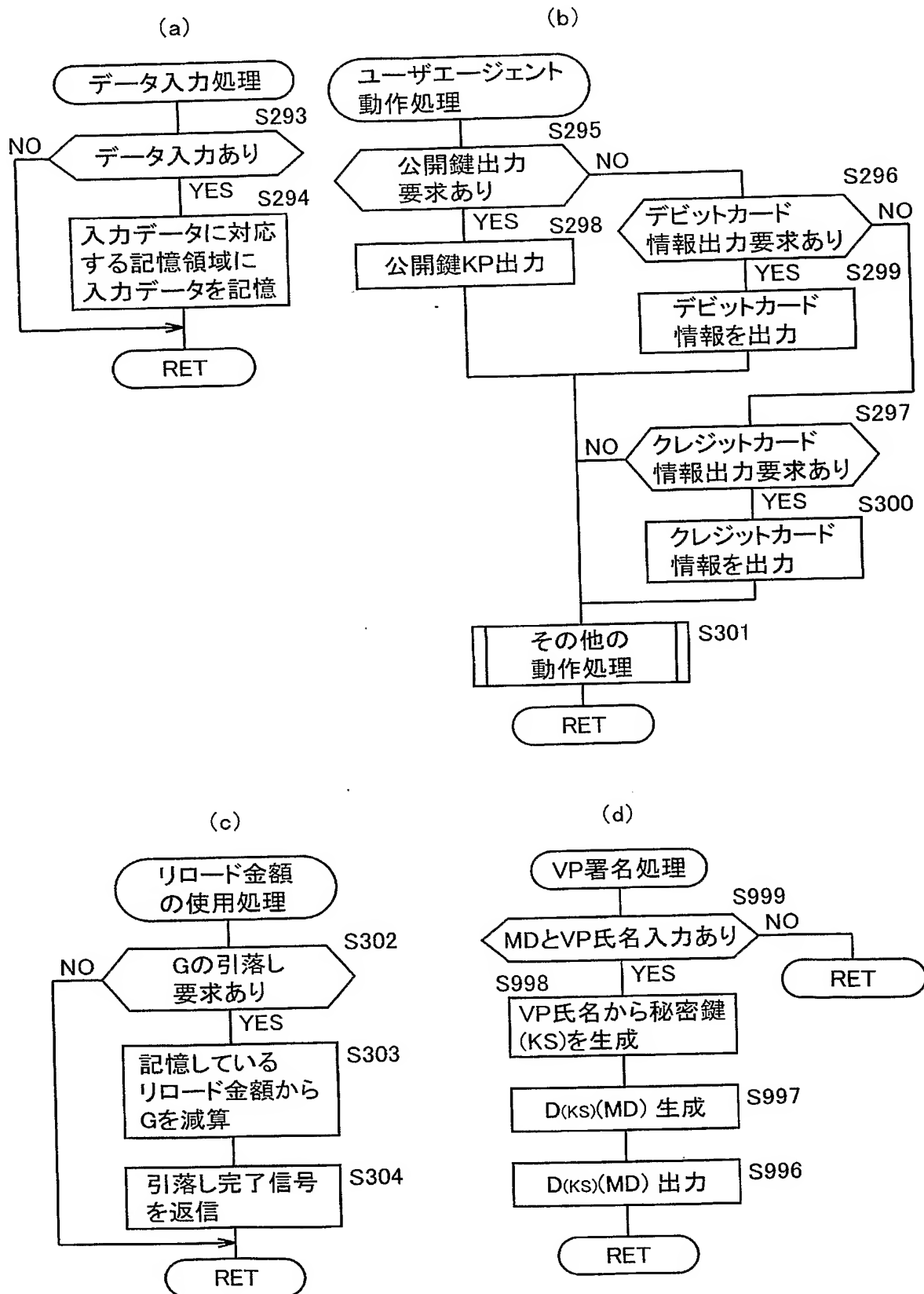
【図 34】



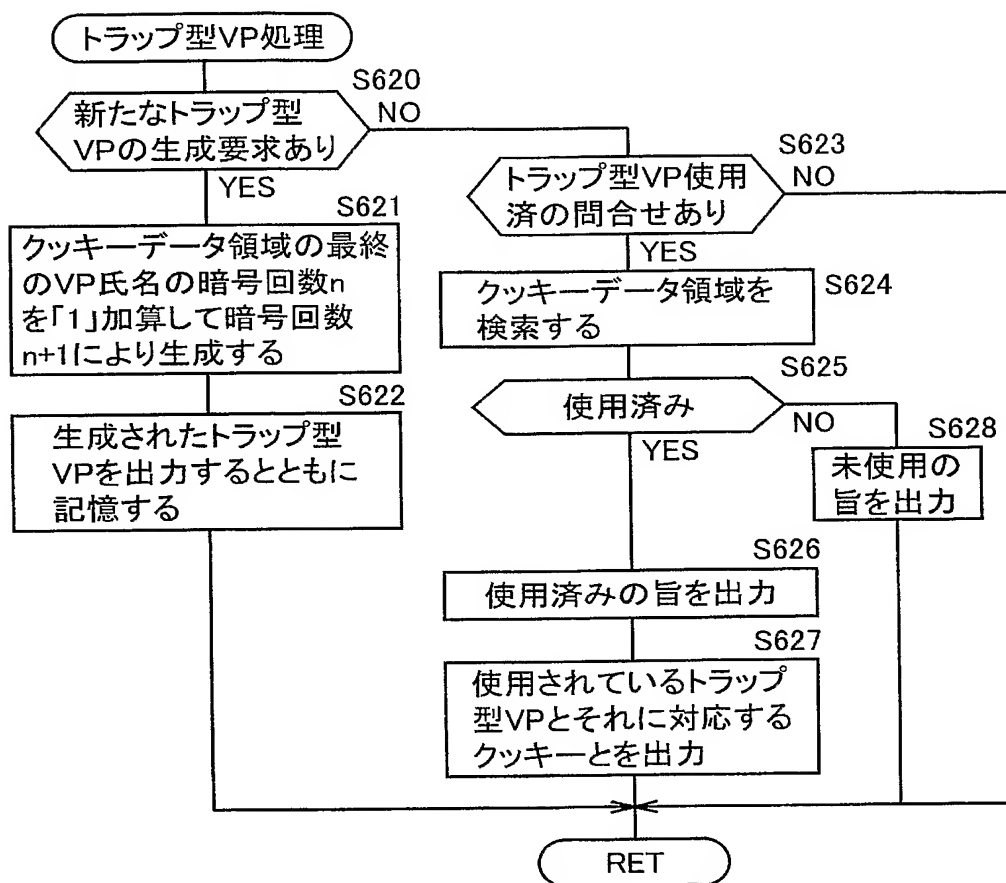
【図 35】



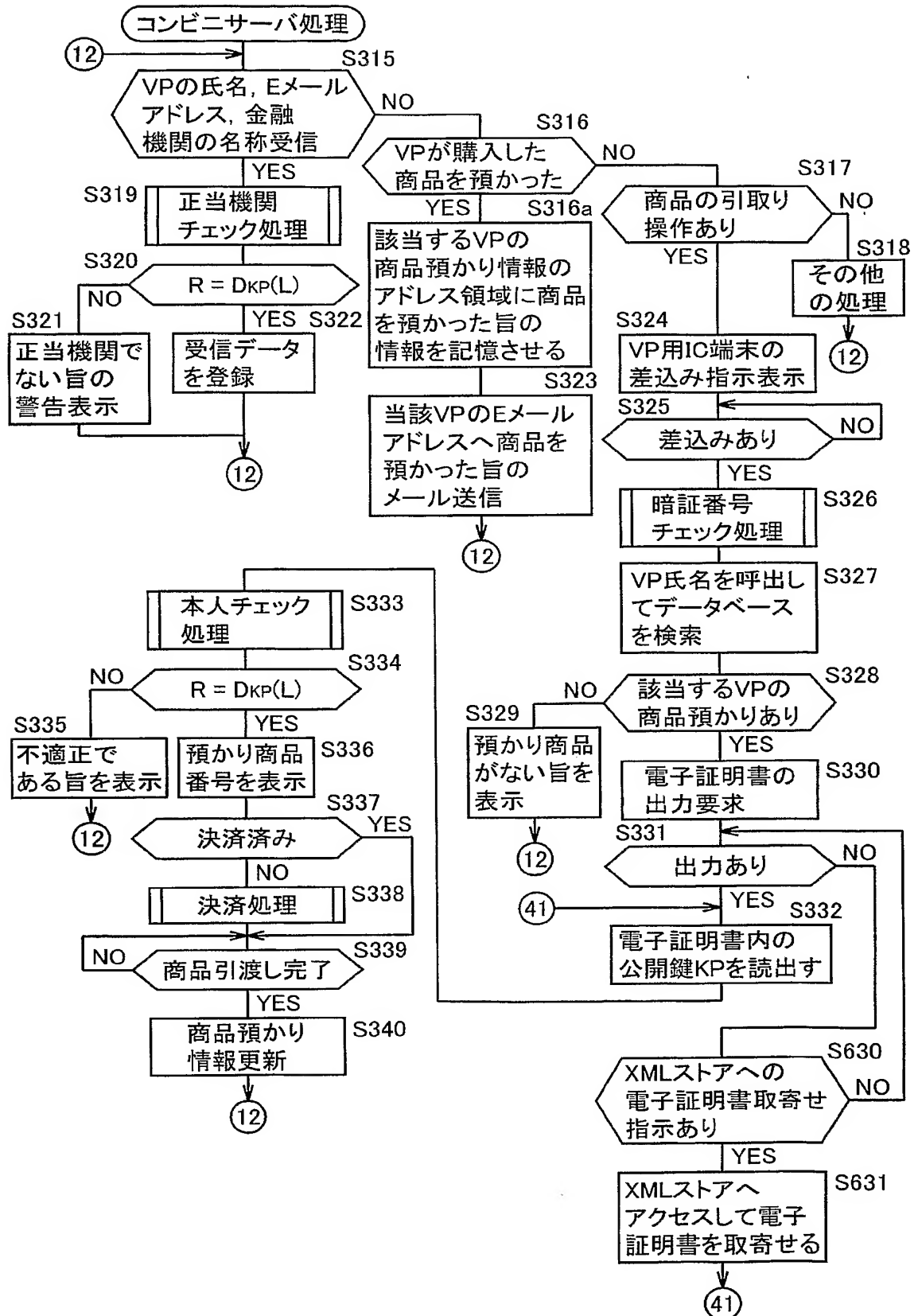
【図 36】



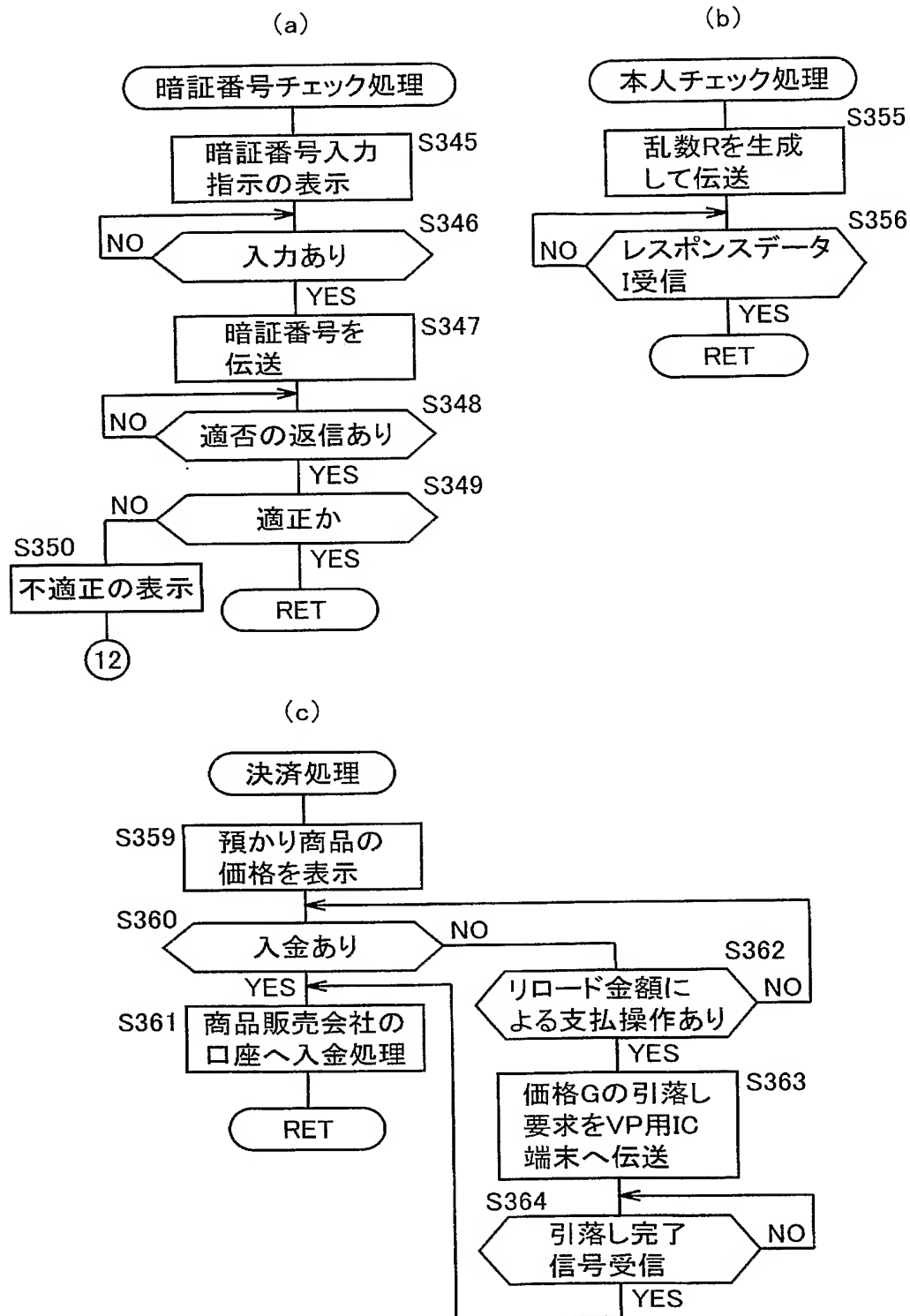
【図 37】



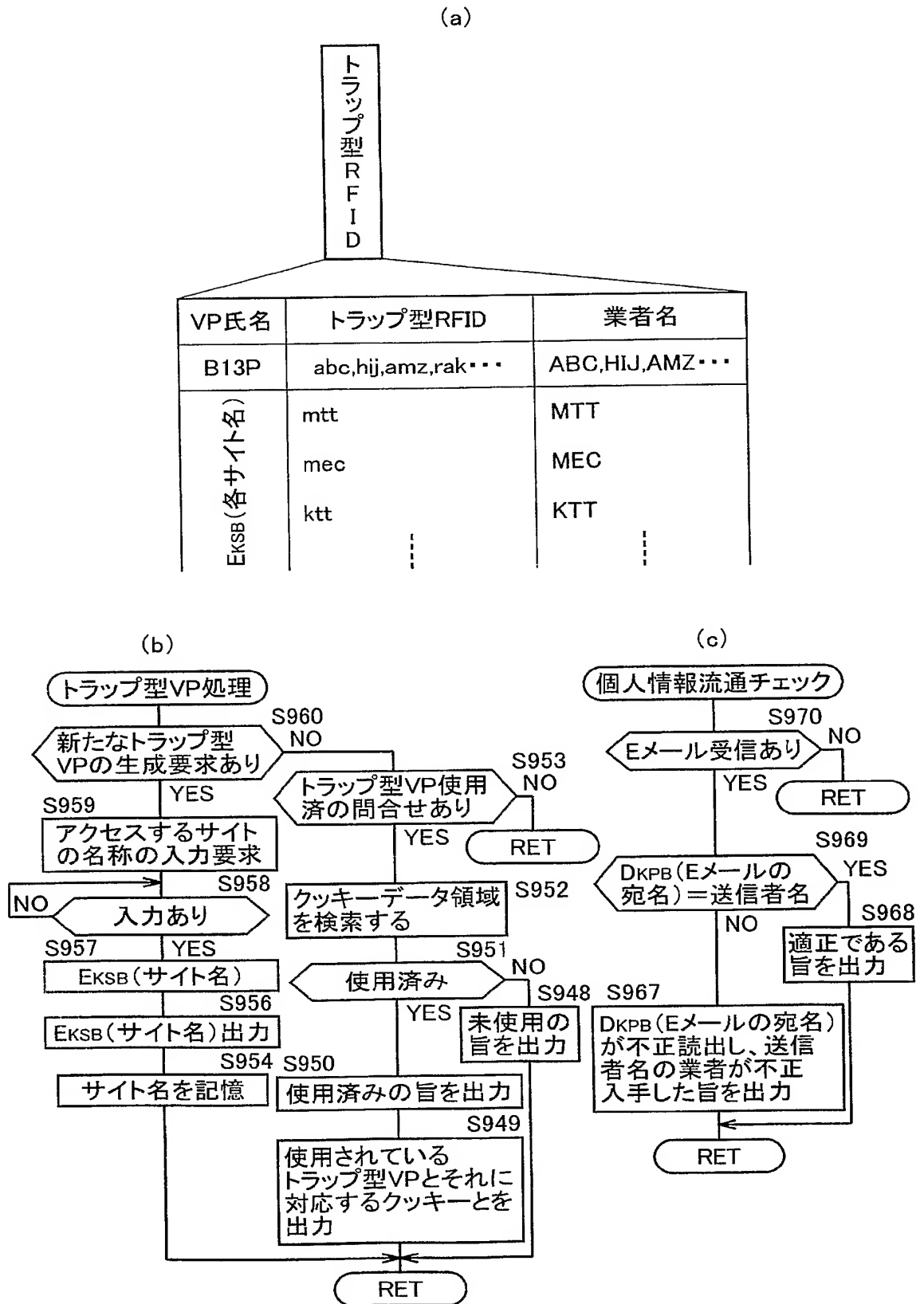
【図 38】



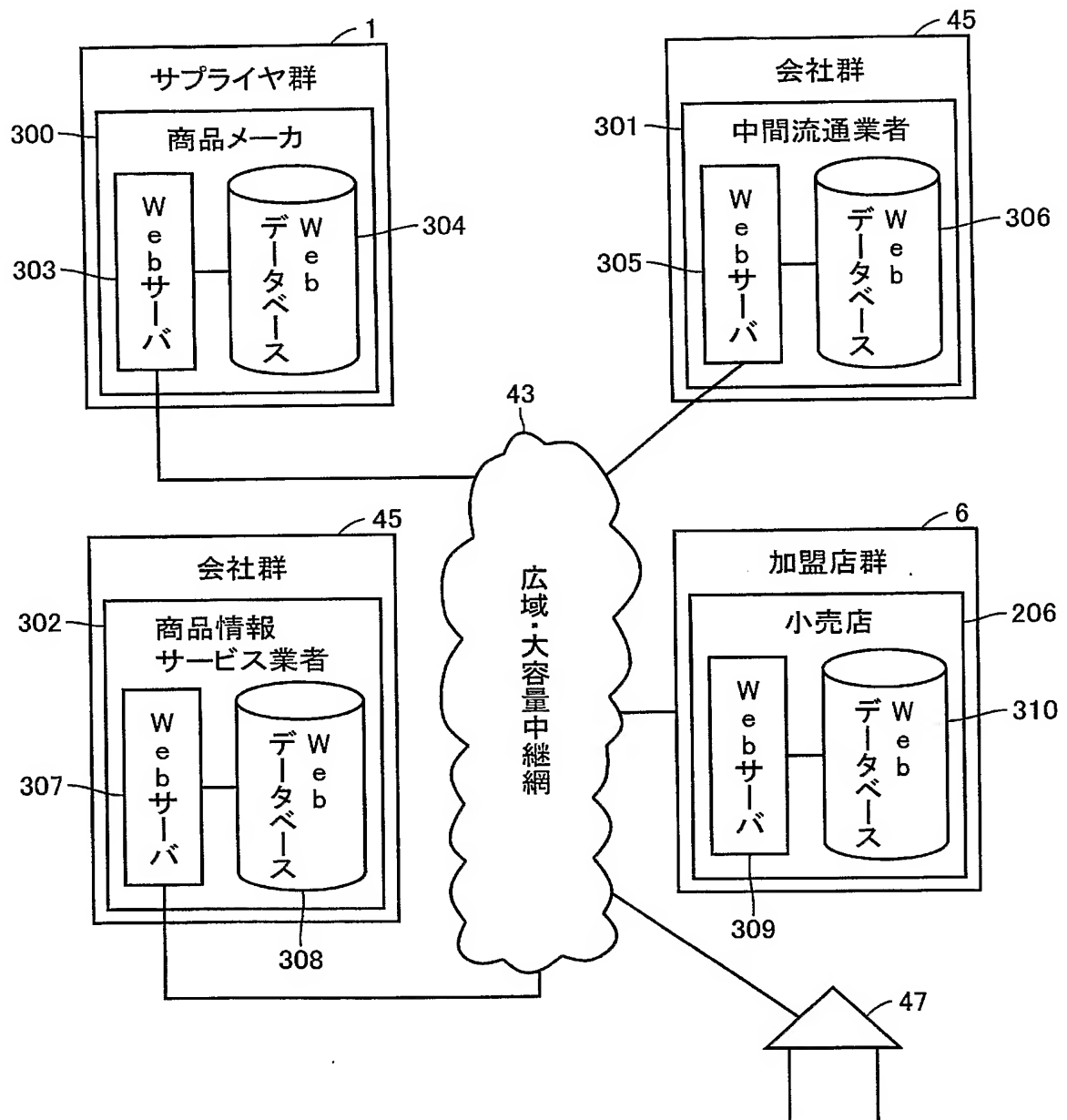
【図 39】



【図 40】



【図 41】

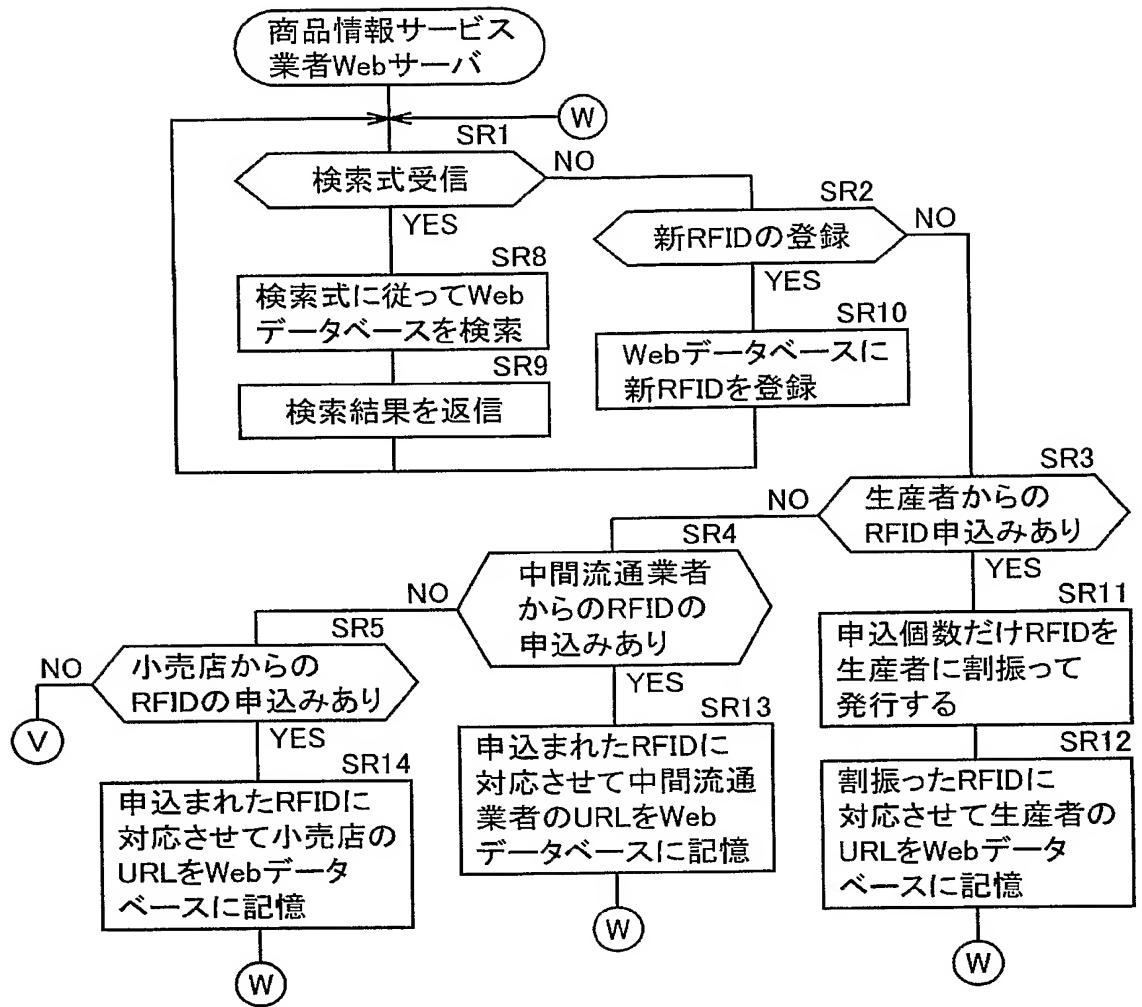




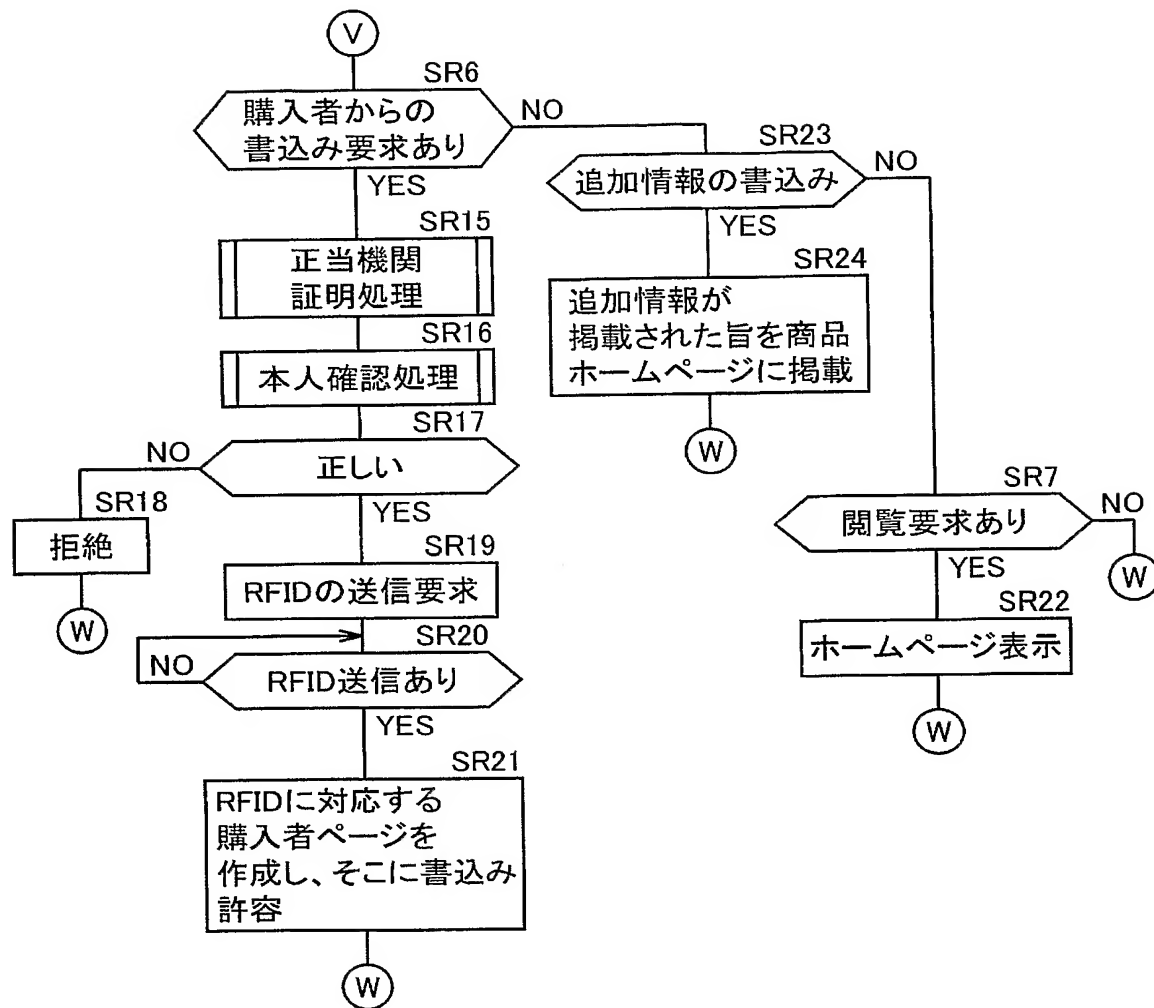
【図 4 2】

RFID	生産者	中間流通業者	小売店	購入者ページ		
892013960	http://www.sato	http://www.kanei	http://www.daimaru	B13P	...	...
892013961				NPXA	...	...
892013962 }				I9X3	...	...
892014560	http://www.isida		http://www.hansin			
892014561 }						
892014801						
892014802 }	http://www.kato	http://www.mitui				
892014990						

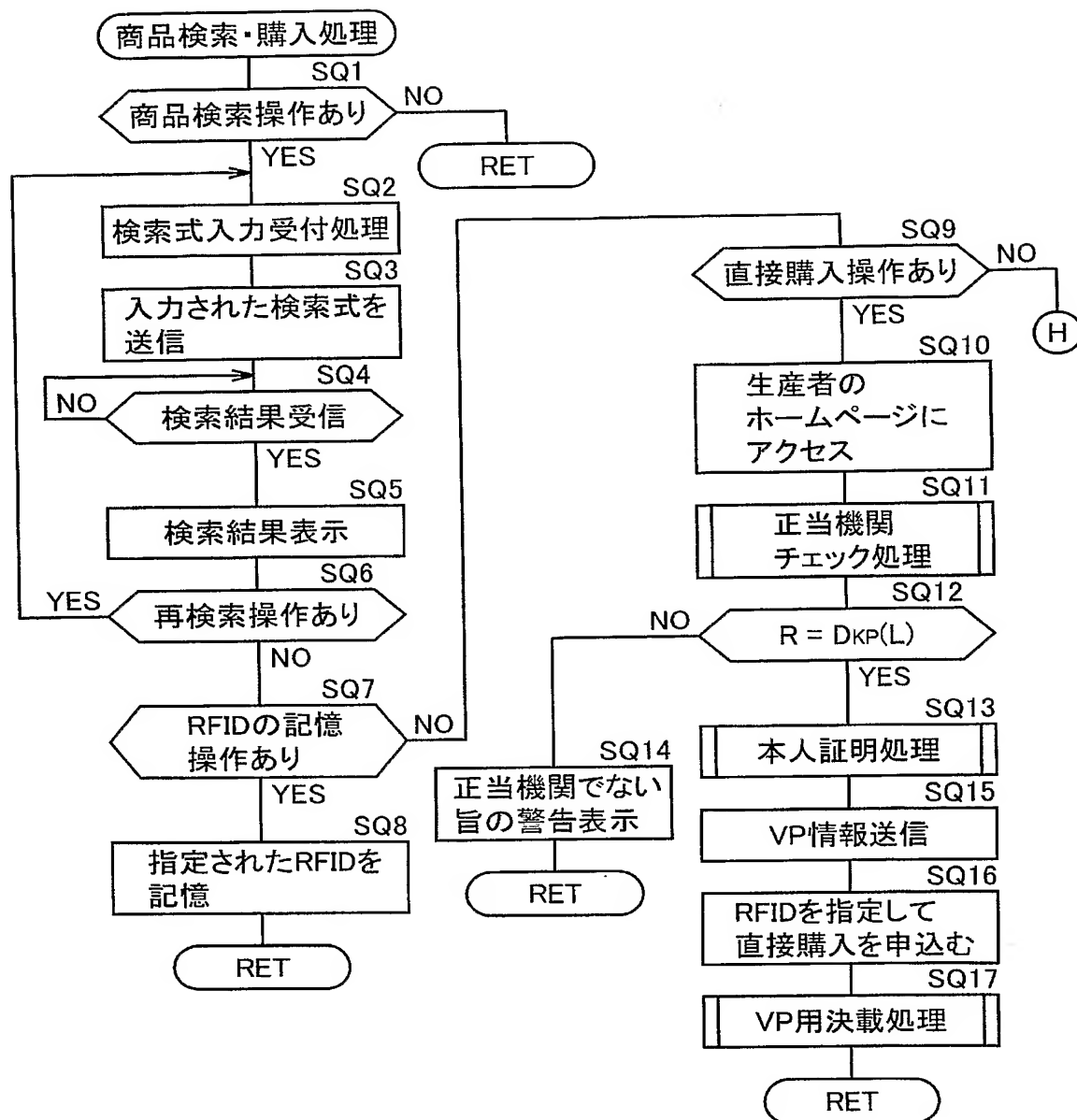
【図 43】



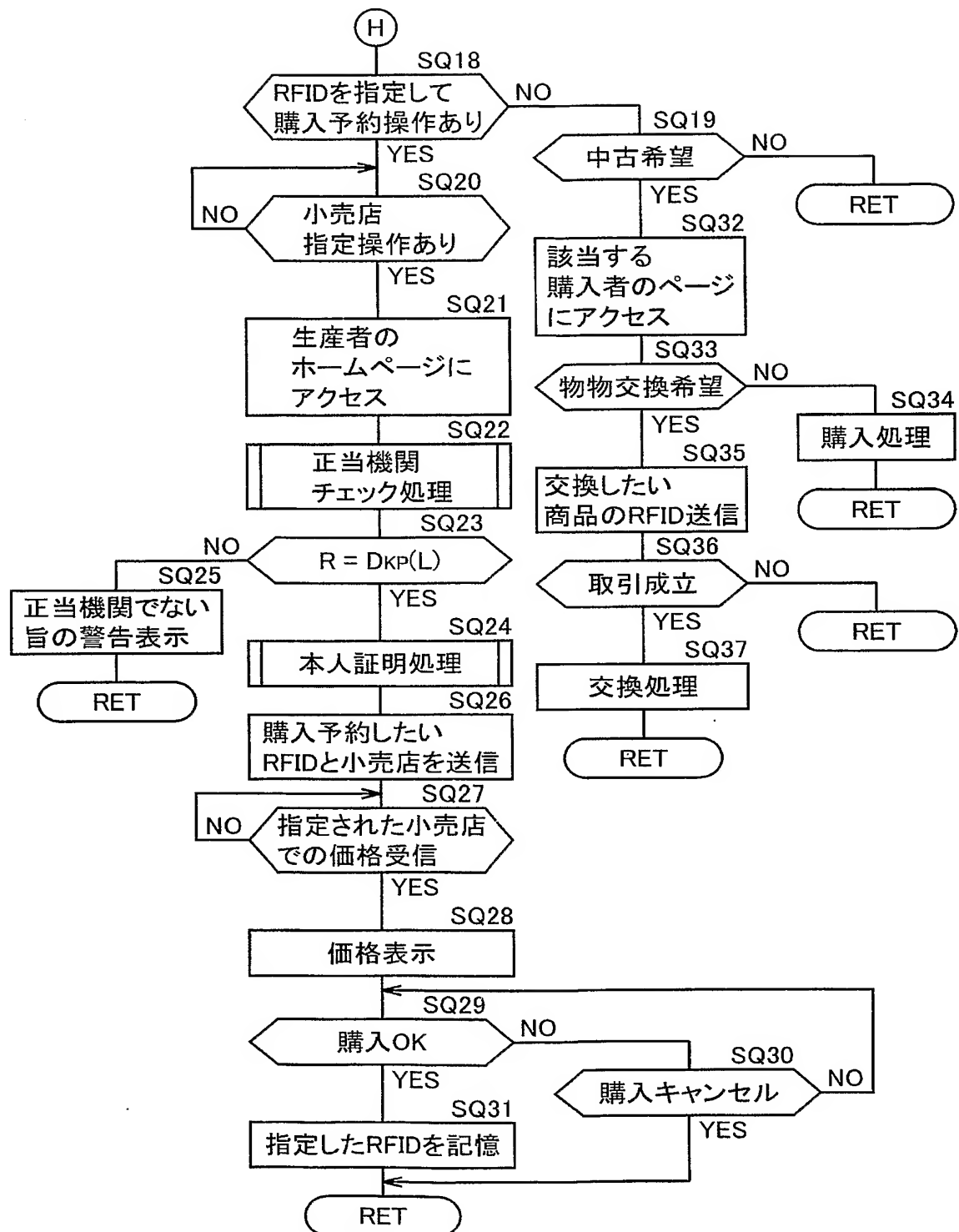
【図 44】



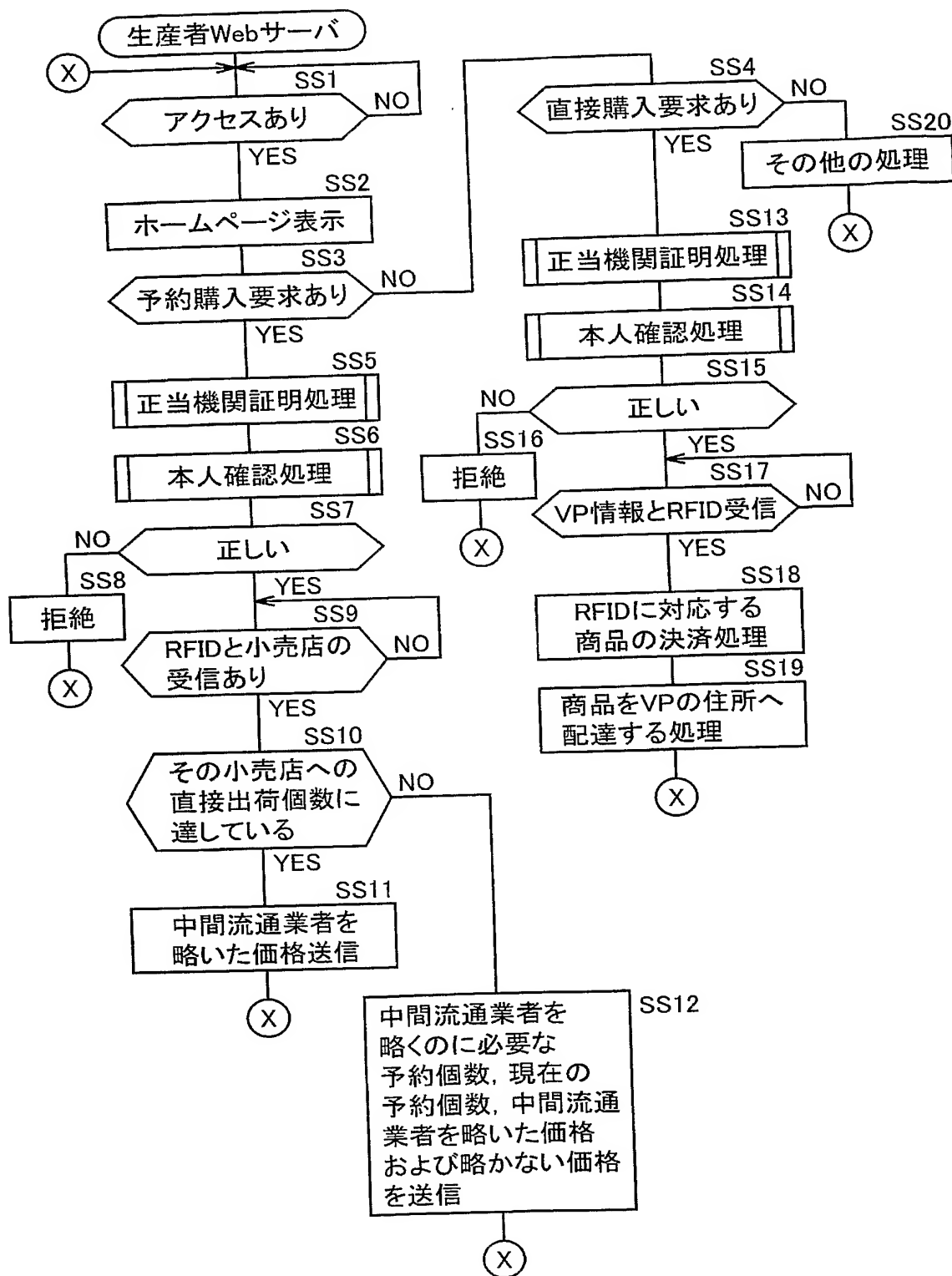
【図 45】



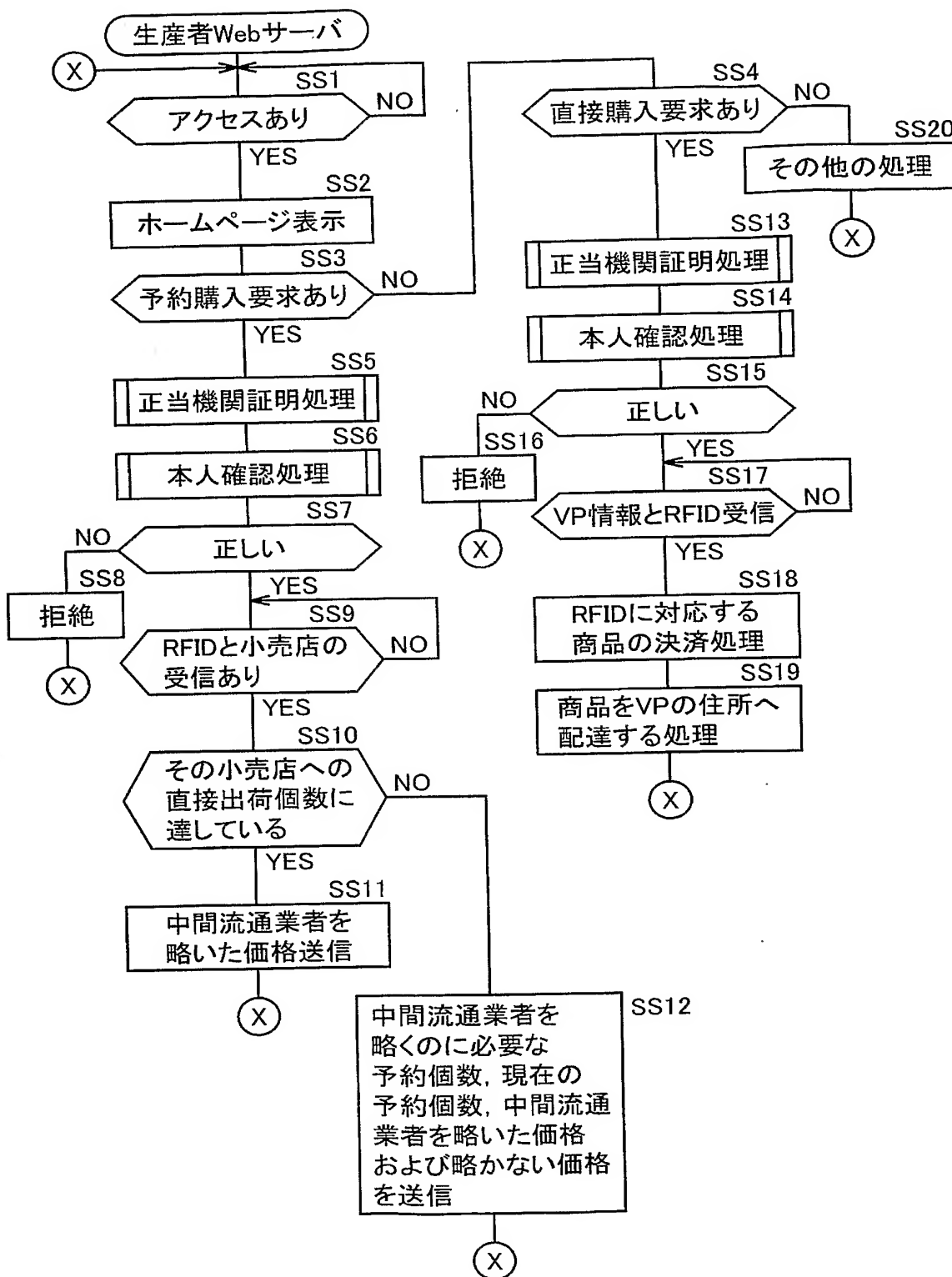
【図 4 6】



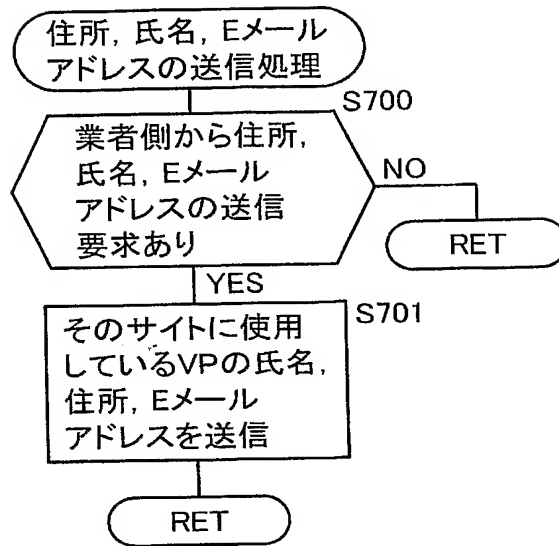
【図 47】



【図 47】

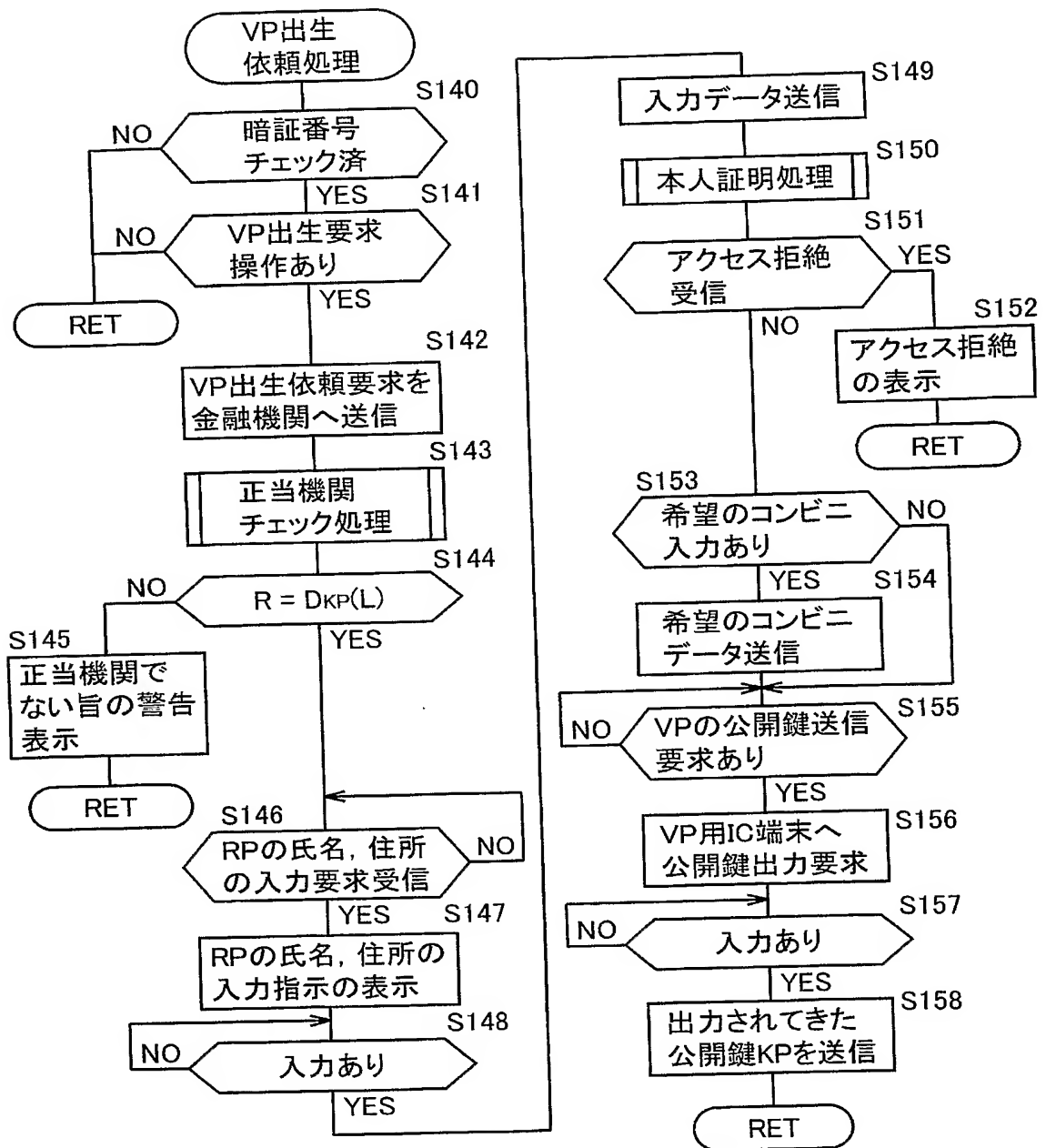


【図 48】

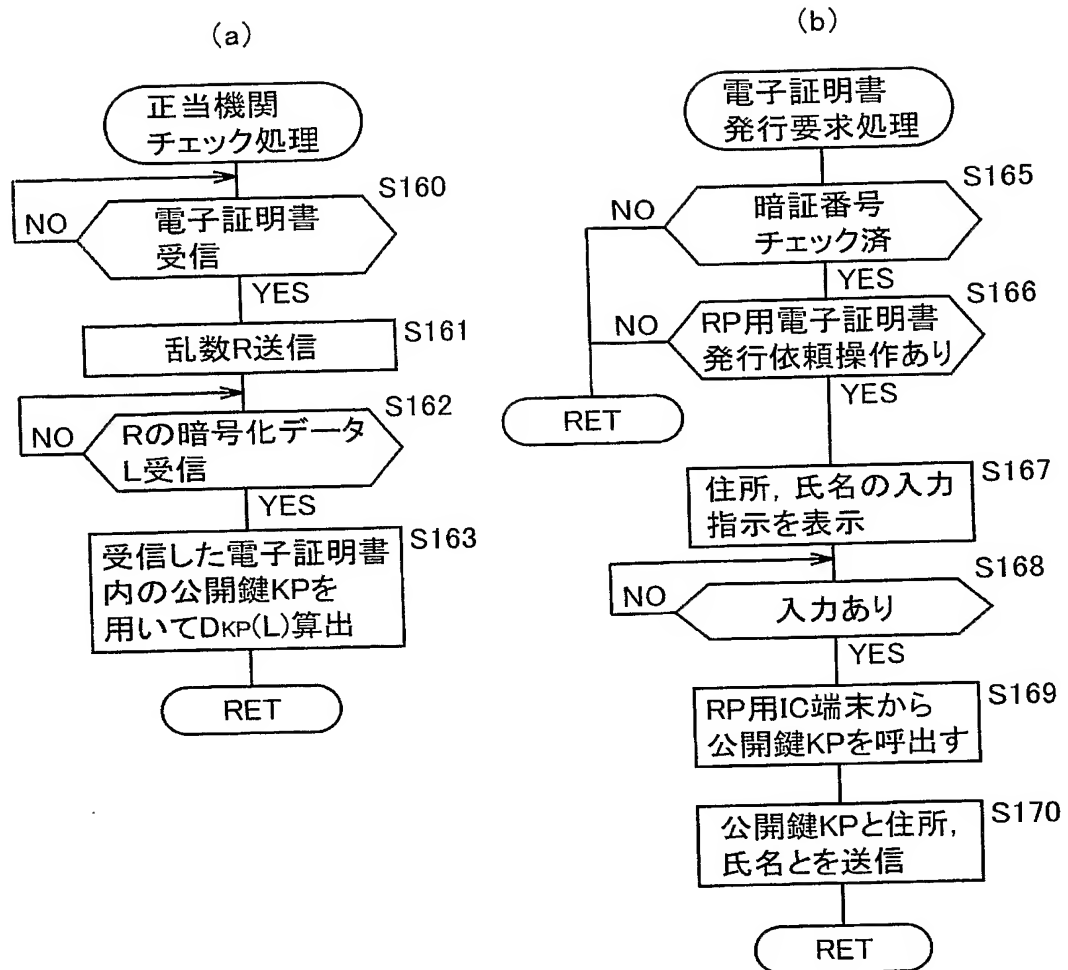




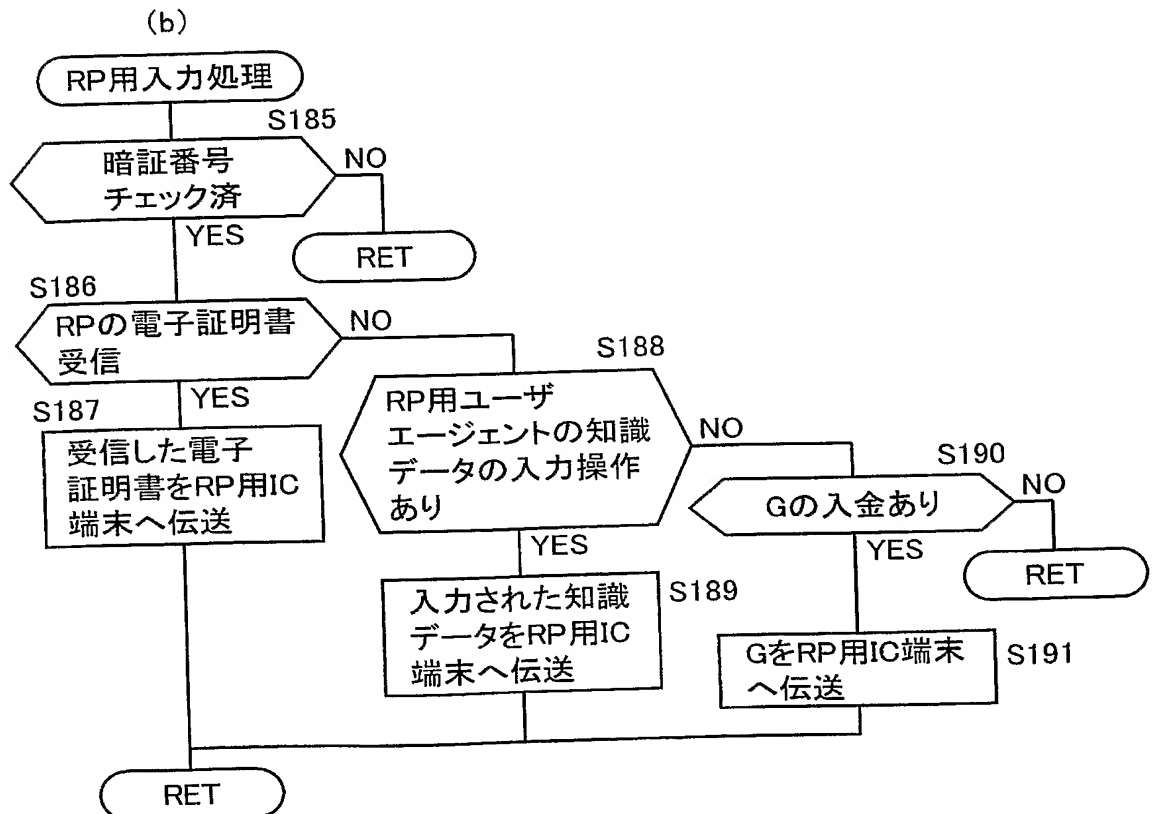
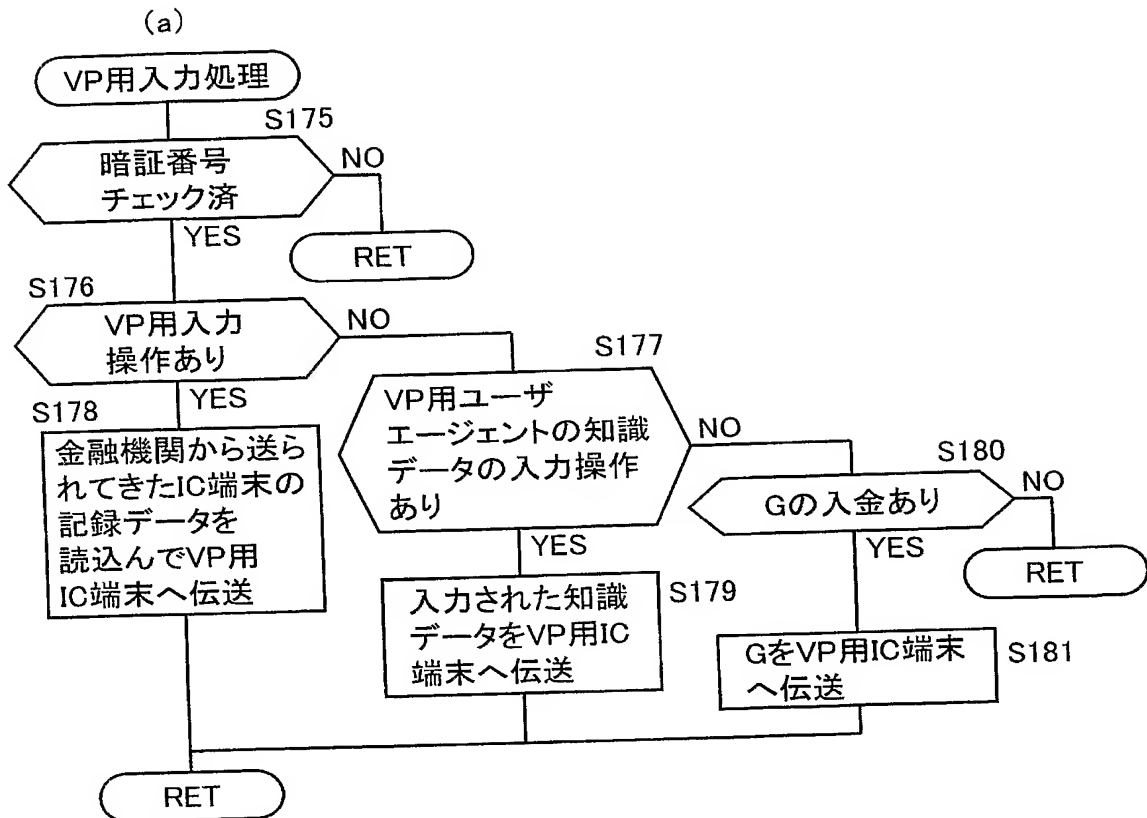
【図 49】



【図 50】

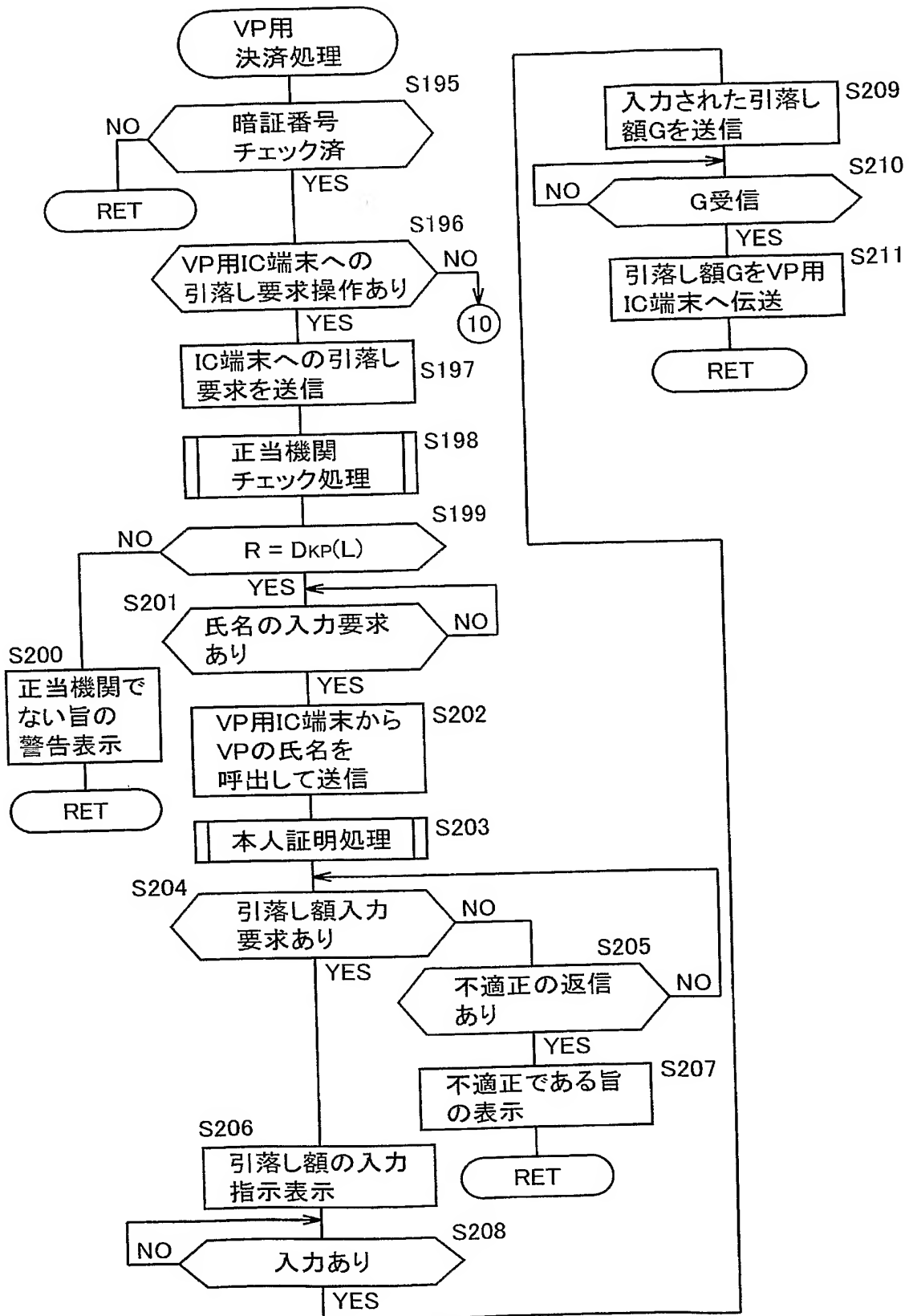


【図 51】

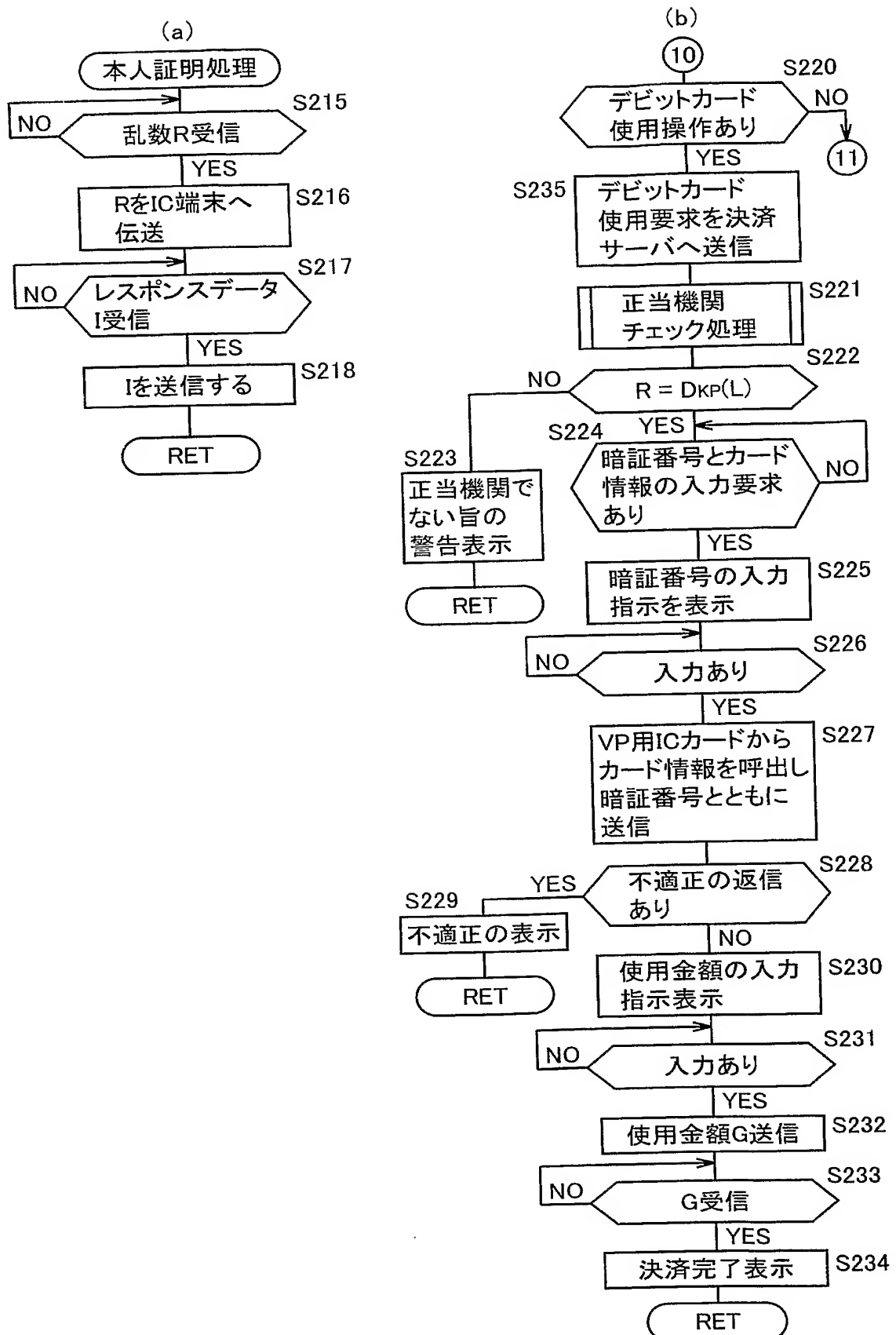




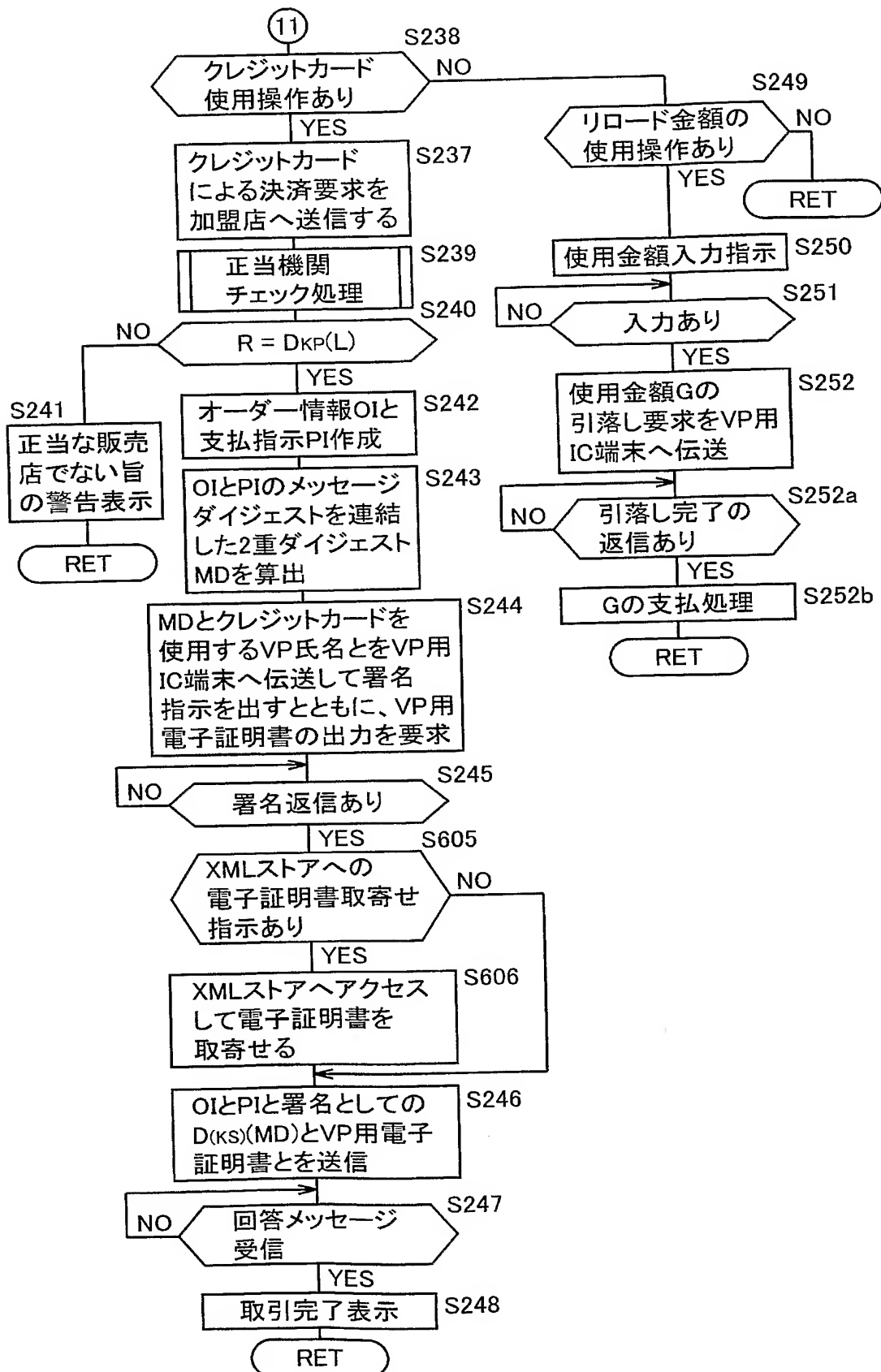
【図 53】



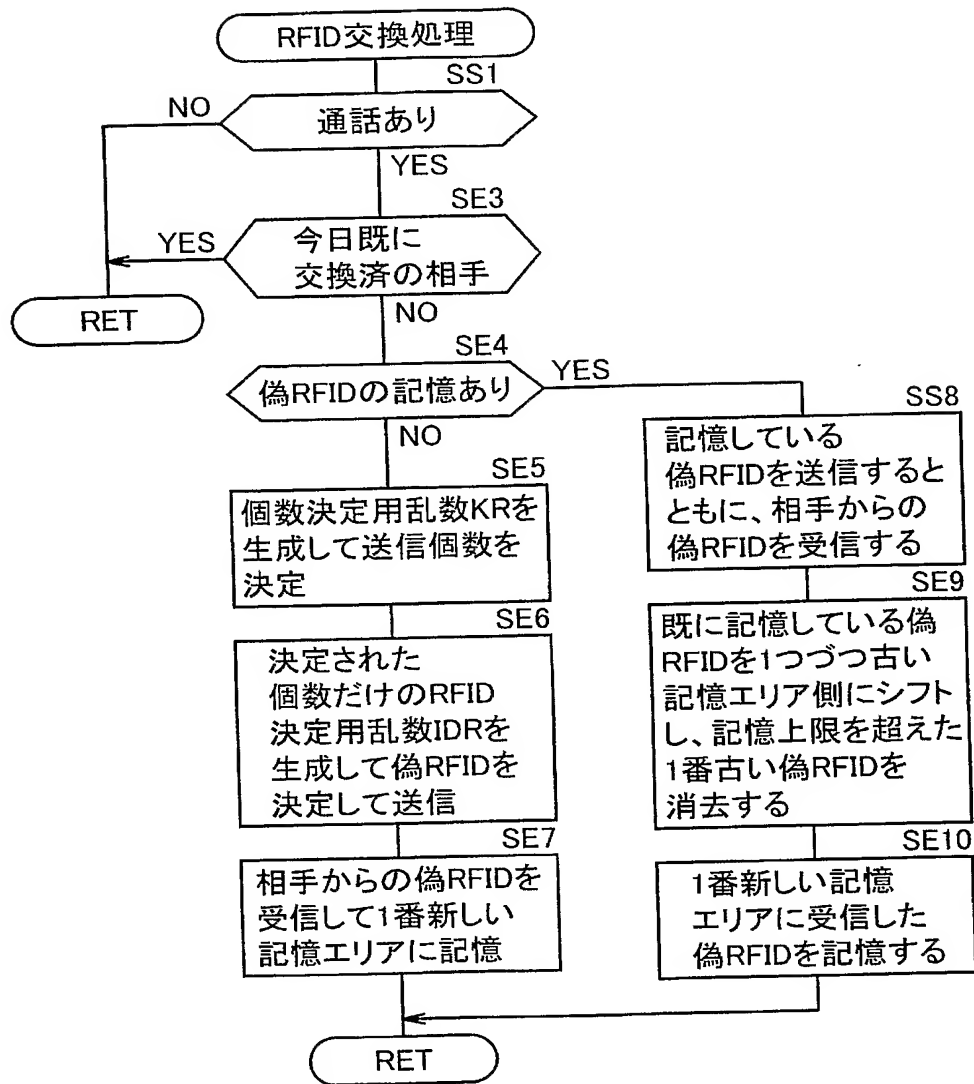
【図 5 4】



【図 55】

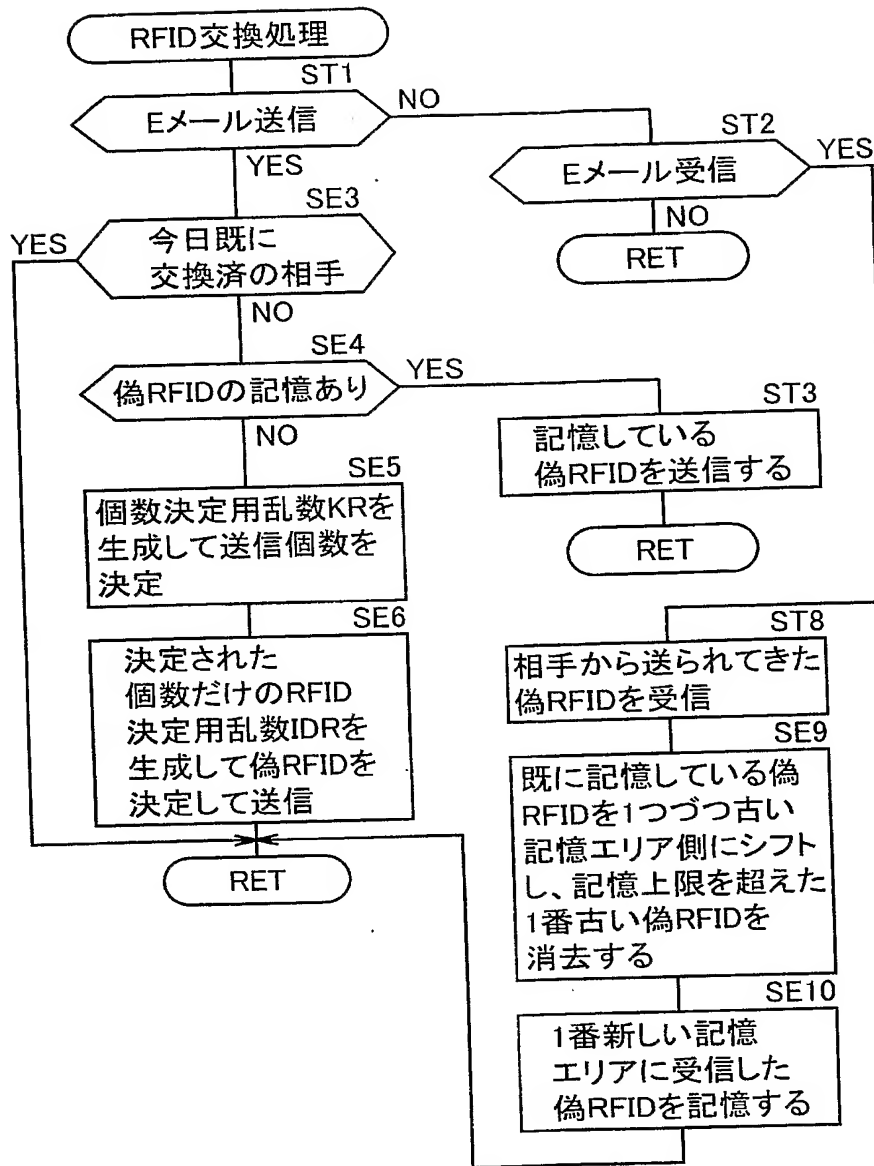


【図 56】

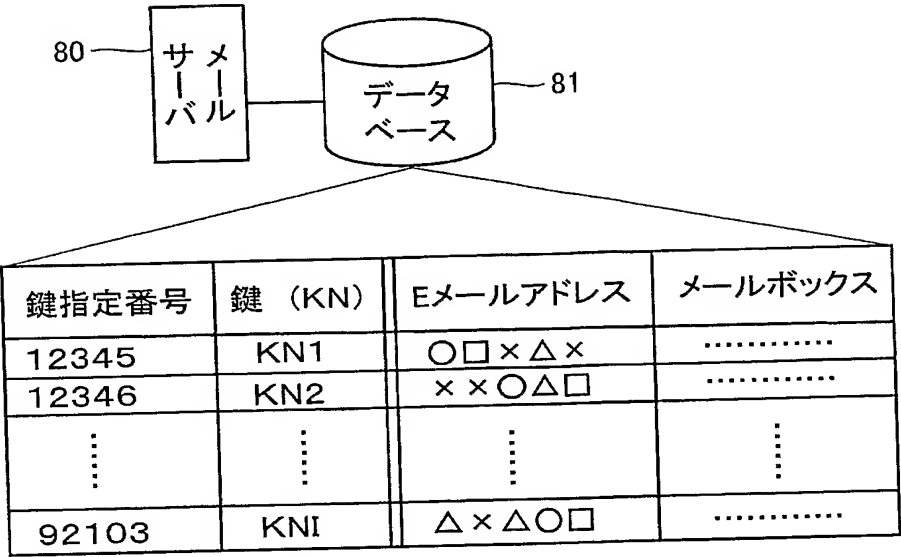




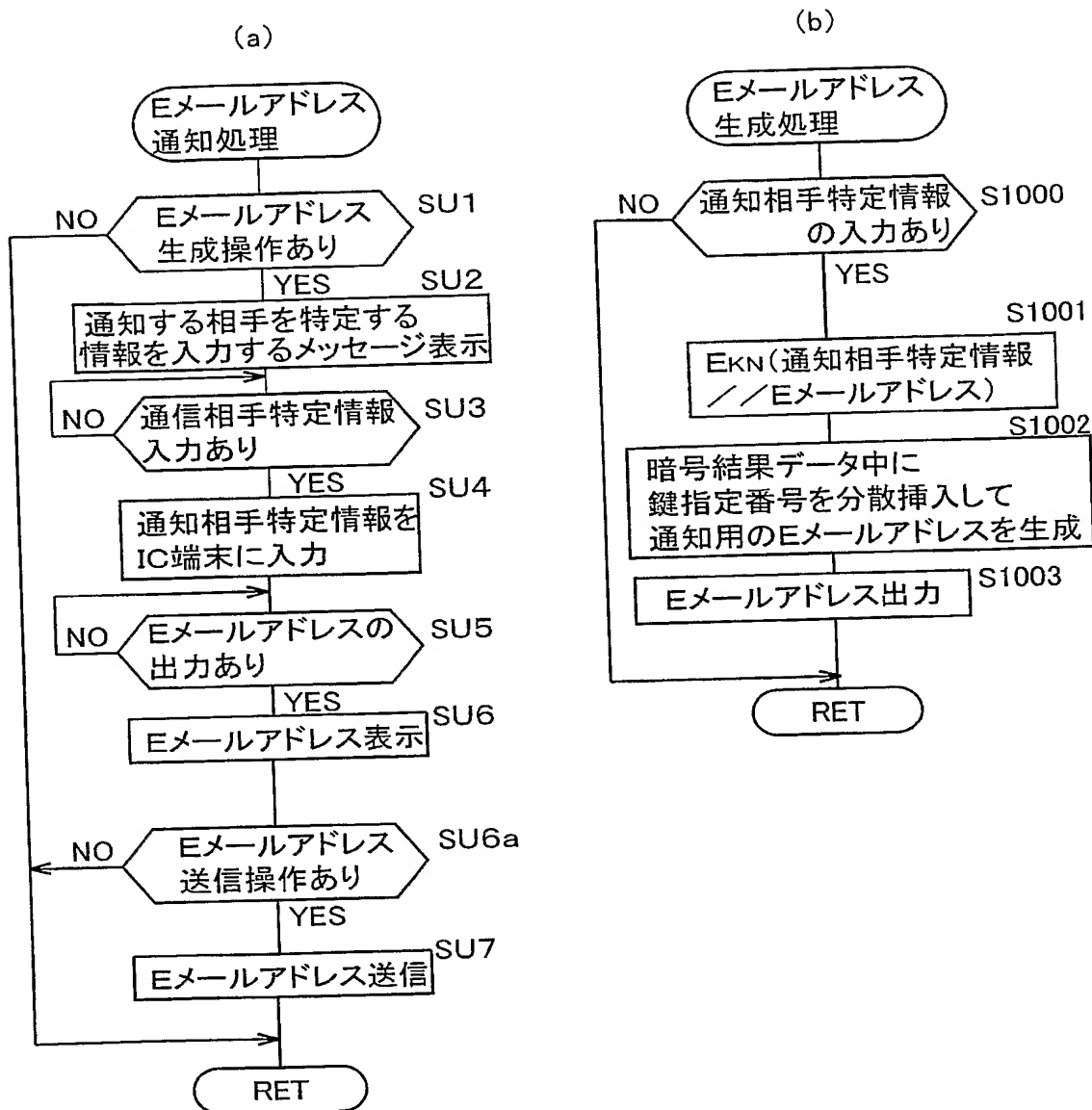
【図 57】



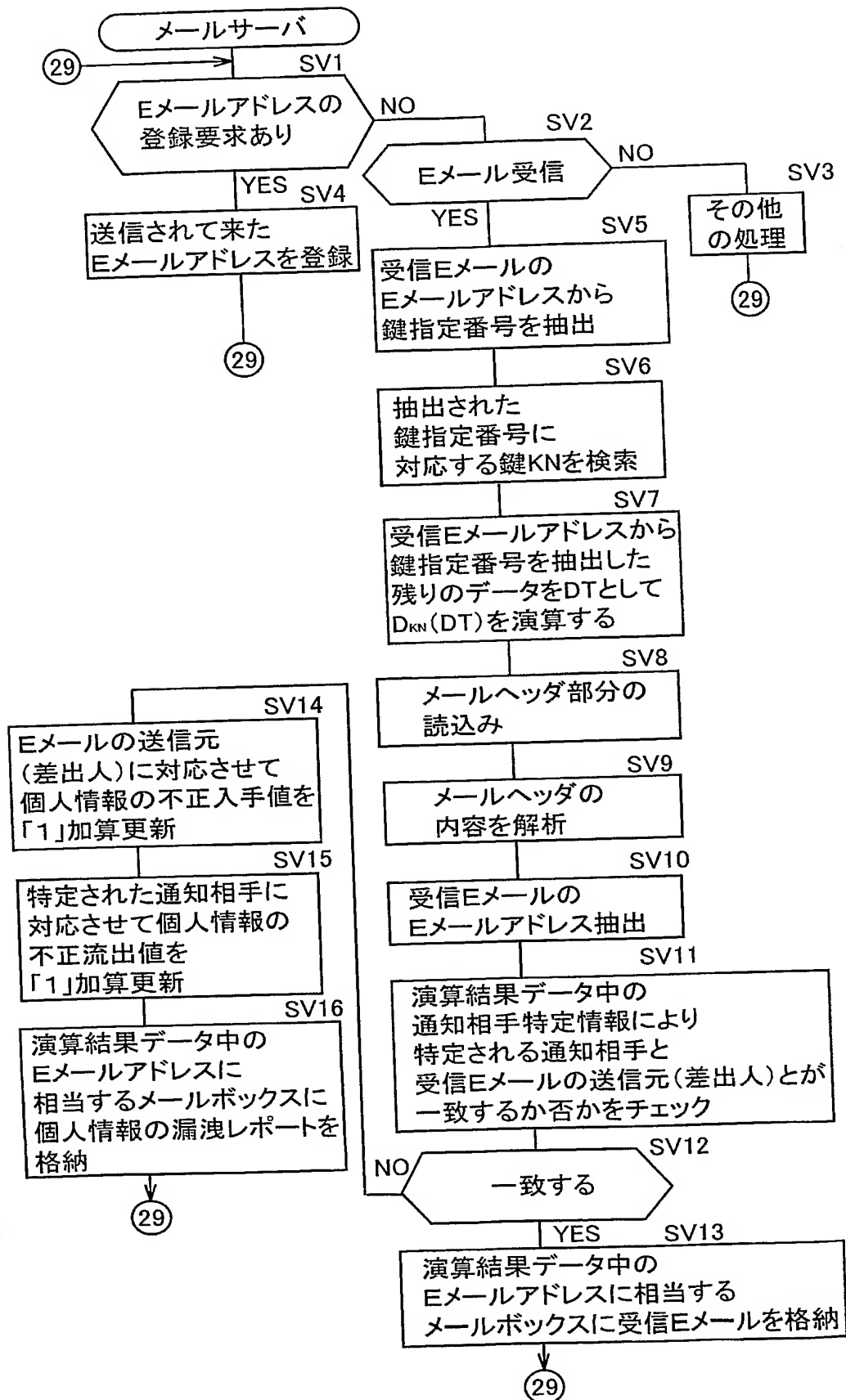
【図 58】



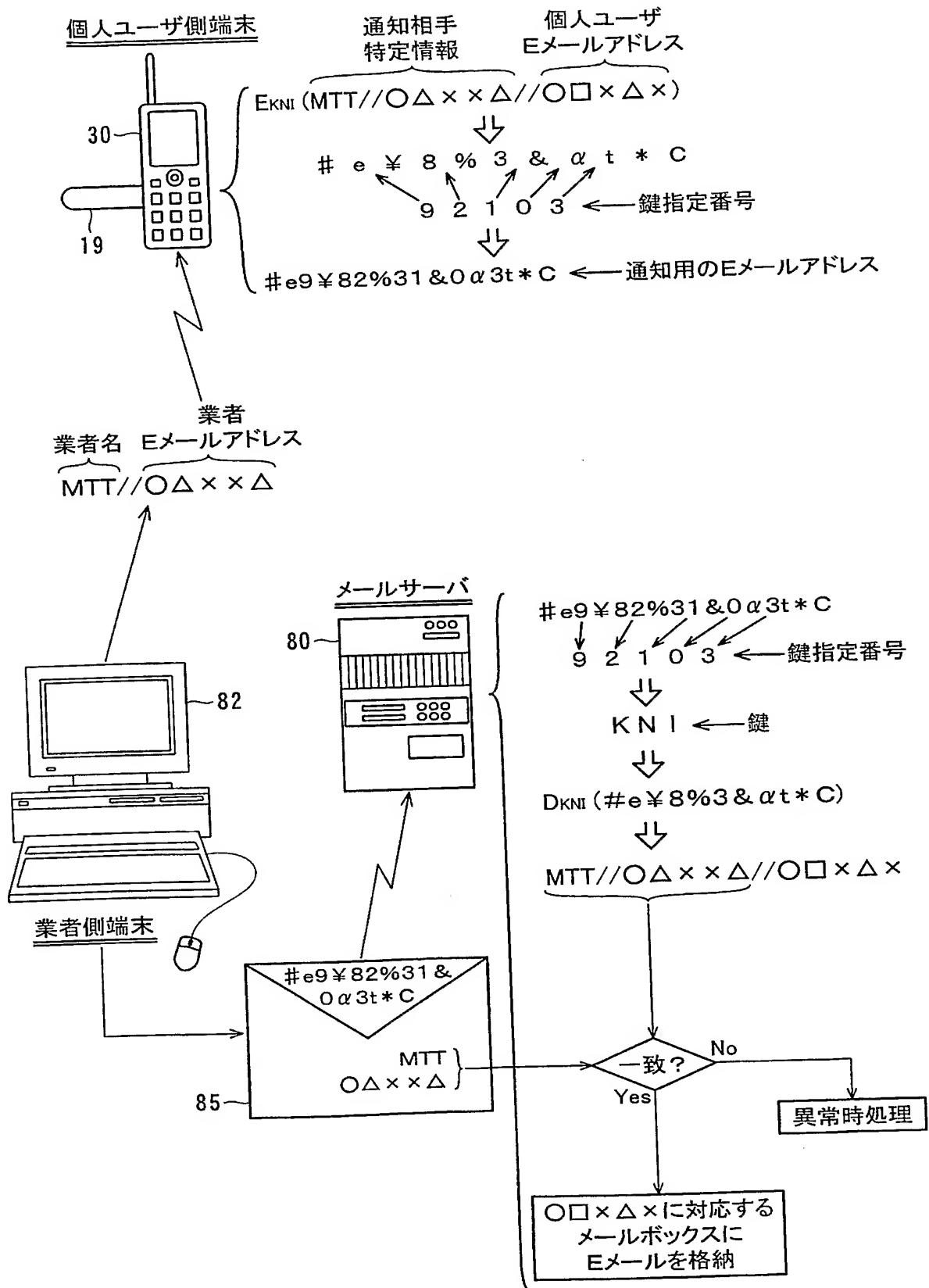
【図 59】



【図 60】



【図 61】



## 【書類名】 要約書

## 【課題】

読取られた固有の識別子に基づいて行われるプライバシーの侵害を防止する。

## 【解決手段】

個人ユーザが業者 M T T に E メールアドレスを通知するにおいて、通知相手の業社名 M T T および E メールアドレスからなる通知相手特定情報と自己の E メールアドレスとを暗号化 ( E K N I ( M T T // ○ △ × × △ // ○ □ × △ × ) ) して通知用 E メールアドレスを生成して通知する。 M T T から R F I D 発信要求があれば M T T 専用の R F I D を発信する一方、 M T T 以外 (たとえば M E C) から R F I D 発信要求があった場合も操作に応じて M T T 専用の R F I D を発信する。その M T T 専用 R F I D とリンクした個人情報が M T T から漏洩した後、 M T T 専用 R F I D を受信した M E C が漏洩個人情報を検索して入手し、その個人情報中の通知用 E メールアドレス宛に E メール 8 5 を送信した場合に、通知用 E メールアドレスを復号して得た通知相手特定情報 M T T // ○ △ × × △ と Eメールの送信元 M E C とが一致せず、個人情報の漏洩元と入手先とを特定できる。

【選択図】 図 6 1

特願 2 0 0 4 - 1 8 2 1 8 0

出 願 人 履 歴 情 報

識別番号

[ 5 0 2 1 7 8 1 2 6 ]

1. 変更年月日

2 0 0 2 年 4 月 9 日

[変更理由]

新規登録

住 所

岡山県倉敷市羽島 2 2 1 番地の 4

氏 名

石井 美恵子